COMMITTEE HANDBOOK

Committee administration and responsibilities of members

Revised November 2022

THE LAW SOCIETY
OF NEW SOUTH WALES

THE LAW SOCIETY
OF NEW SOUTH WALES

COMMITTEE HANDBOOK | REVISED NOVEMBER 2022

1. INTRODUCTION

The Law Society's committees are committees of the Council with powers, authorities and tasks delegated by the Council. They are established as a source of expert advice and assistance to Council, the Society and the profession and are convened annually on the basis of need. Functions vary somewhat from committee to committee but, typically, are as follows:

- a source of policy proposals and reform initiatives;
- a forum for consideration of practical issues and resolution of problems;
- a review body and commentator (in relation to legislation, discussion papers, reports, etc);
- a monitor of practice standards and advocate of ongoing training and skills development;
- a liaison body.

Committees have an important role and the way in which they perform is integral to the professionalism of Council's decision making and the performance of the Society as a whole. Members' participation is critical to the success of committees and is therefore welcomed. (In order to facilitate participation by country-based members, The Law Society of New South Wales offers assistance with travel costs incurred – refer protocol at Appendix 1.)

Committees address a range of issues and can be broadly divided into three categories:

• Policy and practice committees	– for example:	Business Law Family Law
• Liaison committees	– for example:	Revenue NSW/Law Society Liaison
• Regulatory committees	– for example:	Fidelity Fund Management Licensing Professional Conduct

(Task forces or working groups are also convened where there are finite tasks to be undertaken or where there is an agenda which does not necessarily require the ongoing support of a committee.)

The Society ensures that the effectiveness of its committee network is maintained by:

1. an annual assessment of the relevance of existing committees and the need for new committees;
2. providing committees with a balance of necessary skills and knowledge and a dynamic membership;
3. ensuring that committees are manageable in terms of numbers;
4. testing optional structures;
5. maximising profession-wide awareness of and interest in the committees and their role;
6. having a membership broadly representative of the Society's constituent groups and of relevant outside bodies; and
7. requiring that committees prepare papers in accordance with quality principles.

2. APPLICATION OF HANDBOOK TO PCC AND DISCLOSURE CONDUCT

The PCC and Disclosure Committee have separate Constitutions approved by Council, to align with provisions of the Legal Profession Uniform Law Application Act 2014. Members of those Committees must also ensure that they comply with the requirements of those Constitutions, including arrangements around confidentiality and conflicts of interest.

To the extent of any inconsistency with those Constitutions, the provisions of the Constitutions prevail over the provisions of this Handbook. Further, paragraph 7.1 (to the extent it relates to term limits) and paragraph 8 do not apply to the PCC and Disclosure Committees.

3. APPOINTMENT TO COMMITTEES

Committee appointments are made annually for a term of one year. The process is governed by guidelines based on principles of effectiveness and equal opportunity and takes account of statutory requirements.

1. Eligibility

1.1 All NSW solicitors with current practising certificates are eligible for appointment to two of the Law Society's statutory committees – the Licensing and Professional Conduct Committees.

1.2 Solicitor appointments to other committees, including the Fidelity Fund Management Committee, are restricted to members of The Law Society of New South Wales.

1.3 Lay[1] applicants with the requisite skills are eligible for appointment to most Law Society of New South Wales committees.

2. Committee vacancies

2.1 Approximately 25 standing committees of the Council are convened each year and current guidelines set a maximum of 12 to 14 as the optimum committee membership. Although this varies in accordance with need, vacancies are limited, and the number of applications always greatly exceeds available places.

2.2 Vacancies occur as a result of resignations as well as The Law Society of New South Wales' turnover policy.

2.3 Casual vacancies are filled by suitable applicants who were not appointed due to lack of vacancies at the time of application, or by a new nominee if the vacancy is the result of a departing representative.

3. Recruitment

(Dates are indicative only)

3.1 In September each year, the Society invites expressions of interest in the committees via a notice to the profession included in Monday Briefs and published on The Law Society of New South Wales website. All interested practitioners, including current committee members, are asked to complete a short form and to provide brief details pertinent to their eligibility for the appointments sought.

3.2 Expressions of interest in appointment are also sought from lay persons whose participation in the work of the committees may be required under the Legal Profession Uniform Law (NSW) or who have particular skills and expertise useful to the work of other committees.

3.3 Appointments to the Ethics Committee are restricted to members of The Law Society of New South Wales.

4. Selection process

(Dates are indicative only)

4.1 During November, an Executive Panel comprising the President Elect (Chair), President, Junior Vice President, two non-Executive Councillors rotated annually, and supported by staff is convened to carry out the selection process.

4.2 When making its selections, the Panel takes into account, as far as is feasible, the balance on the committee in terms of relevant expertise, representation of the Society's constituent groups and outside organisations, and gender.

4.3 Members are advised of the outcome of their applications during December.

5. Chair

5.1 The best candidate will be the Chair, whether he/she is a Councillor or non-Councillor. Where a non-Councillor is appointed Chair, a Councillor may be appointed a member of the committee.

---

1. According to the legal profession legislation (as defined in the *Legal Profession Uniform Law Application Act 2014*, a lay member is a person who is not an Australian lawyer (i.e. has not been admitted in Australia).

6. Representatives of Outside Bodies

6.1 In addition to members selected from the legal profession, committees may also include representatives of outside bodies such as government departments, the courts, other professional associations and so on. This provides committees with a range of relevant perspectives and expertise on matters under consideration.

6.2 Whether a particular Committee needs representatives from any given organisation is a matter for the President of the Law Society, acting on the advice of the relevant Law Society Department, and the Chair and Deputy Chair of the Committee.

6.3 Representatives are appointed personally, and whether an alternate can attend in the representative's place is a matter to be determined by the Chair on a case-by-case basis.

7. Period of appointment

7.1 Committee members are appointed for one calendar year, but may have up to three consecutive appointments.

7.2 Reappointment is not automatic. It depends on a number of factors including the member's contribution to the work of the committee (see "Responsibilities of Committee Members", p.8).

8. Reappointment

8.1 In order to allow as many interested Society members as possible to serve on committees and to facilitate the regular introduction of new ideas, tenure is generally limited to a maximum of three consecutive years.

8.2 Committee tenure can be extended to a maximum of five consecutive years if, at the time of selection, the Executive Panel is satisfied that an extension beyond the preferred three-year tenure is justified.

8.3 In order to facilitate ongoing membership of practitioners with unique expertise or skills, where appropriate committees are allowed two quarantined positions – that is, positions free of any tenure restrictions.

8.4 Periods of appointment of representatives of outside bodies are subject to consultation from time to time with the nominating body.

8.5 Tenure restrictions do not apply to lay members fulfilling a role required under the Act.

8.6 Chairs are appointed to Policy and Practice and Liaison Committees for a maximum period of four years.

9. Termination of appointment

9.1 A member is free to resign his/her committee appointment at any time. (See also clause 6, "Responsibilities of Committee Members", p. 8).

9.2 In the absence of extenuating circumstances, a member's appointment can be terminated by the President of The Law Society of New South Wales if he/she has failed to attend three meetings and/or is regularly unable to complete allocated tasks (see clause 3.3, "Responsibilities of Committee Chairs", p.7).

9.3 A committee member's appointment will be terminated by the President of The Law Society of New South Wales if his/her practising certificate is cancelled or suspended as a consequence of a regulatory issue.

10. CPD Units

10.1 Refer to Legal Profession Uniform Continuing Professional Development (Solicitors) Rules 2015.

8.1.4 membership of a committee, taskforce or practice section of a professional association, designated local regulatory authority or the Law Council of Australia or of other committees, provided that the solicitor regularly attends its meetings, if the work performed on the committee, taskforce or practice section is of substantial significance to the practice of law and is reasonably likely to assist the solicitor's professional development.

9.1 CPD unit means:

9.1.3 in relation to a CPD activity referred to in rule 8.1.4, two hours of the activity.

9.2 in calculating the relevant CPD units of CPD activity in respect of a CPD year, the total must not include:

9.2.3 more than 3 CPD units of CPD activity referred to in rule 8.1.4.

4. COMMITTEE MEETINGS

1. Most Law Society of New South Wales committees meet monthly or bimonthly. Some meet more often (for example, the Professional Conduct Committee meets fortnightly), and others less often.
2. Meeting schedules for the year are settled as soon as possible after Committee recruitment is completed and circulated to members.
3. Meetings are held at The Law Society of New South Wales' premises, 170 Phillip Street, Sydney, or via teleconferencing or videoconferencing on an as needs basis. Meetings are generally held between 12.00 noon and 2.00 pm if possible, or outside business hours.
4. Duration of meetings is approximately 1.5 hours.
5. The quorum for all committee meetings is three. In the case of statutory committees, there are particular requirements under the Legal Profession Uniform Law (NSW) regarding membership and meetings.

The following sections on responsibilities provide additional information in relation to administrative matters associated with committee meetings.

5. RESPONSIBILITIES - GENERAL

1. Confidentiality

1.1 All committee members are expected to observe strict rules of confidentiality with respect to committee business. They must be conscious that from time to time

- they may be given the opportunity to consider and comment on highly sensitive documents relevant to the committee's specific field released to the Society by government and other authorities;
- they may also be given the opportunity to consider draft policy proposals intended for debate within the committee which should not be presumed to reflect approved Law Society of New South Wales policy relevant to the committee's specific field;
- they may have before them information which may affect the reputation and livelihood of solicitors and other members of the community.

1.2 Any breach of confidentiality could materially affect individuals; or damage the trust which exists between The Law Society of New South Wales and a number of institutions and organisations; or create false impressions about Law Society of New South Wales policy. It is therefore the responsibility of all committee members to maintain the security of business papers with which they have been provided and to treat as strictly confidential any information to which his or her membership of a Society committee has provided access.

1.3 Where a committee member has been appointed to a Policy & Practice committee as a representative of another organisation, including Young Lawyers –

- the requirement for confidentiality is not intended to prevent the representative member from reporting to his/her organisation general information about the committee's activities. If the representative member wishes to make a more detailed report on a particular issue, he/she should check with the committee's policy lawyer;
- the representative member must maintain the confidentiality of all documents circulated to committee members by Law Society staff or other committee members, including draft submissions, agendas and minutes. If a representative member believes it would be beneficial to share a document with his/her organisation, a request should be made to the committee's policy lawyer.

1.4 The provision made at 1.3 above does not apply to the Law Society's regulatory committees (including Ethics and Costs) where strict confidentiality must be maintained at all times. In particular, the confidentiality provisions of the Legal Profession Uniform Law (NSW) apply to the discharge of statutory responsibilities.

2. Powers and authorities

2.1 The powers and authorities of the Society's committees are delegated by the Council. It is the responsibility of all committee Chairs and members to act within the parameters of these delegated powers and authorities.

3. Media

3.1 Only The Law Society of New South Wales' President and the Chief Executive Officer are authorised to speak to the media on behalf of The Law Society of New South Wales. If speaking to the media, committee members must not imply or allow it to be inferred that they are speaking on behalf of The Law Society of New South Wales or its committees. The only exception to this is if they have the specific authority of the President or the CEO to do so.

3.2 Any enquiries concerning The Law Society of New South Wales that are raised with committee members directly should be passed in the first instance to the Society's Media and Public Relations Manager on 02 9926 0288.

4. Tasks

4.1 Committees' primary responsibilities for the year are tasks determined by the needs of Council. Some tasks are included in the directives approved by Council each year and others arise during the year.

5. Participation in the work of the committees

5.1 Membership of the Society's committees is voluntary and unpaid. However, the value of committees' contribution to the profession is a product of members' commitment to the tasks at hand.

6. Copyright

6.1 The Law Society of New South Wales will be the sole and exclusive owner throughout the world in perpetuity of all materials, including all papers and recordings and including all intellectual property rights in such materials, prepared for it by committee members as part of their committee responsibilities including for the following purposes:

- to reproduce such materials; and
- to commercially exploit such materials, including by way of sale or hire.

6.2 Committee members will sign any documents which The Law Society of New South Wales may request to confirm the assignment to The Law Society of New South Wales of copyright in the materials.

7. Quality principles

Documents to be submitted to Council or to outside bodies must be in accordance with the Law Society's commitment to quality principles. Adherence to this guideline is the shared responsibility of committee Chairs, members and staff.

7.1 **Content**

Reports and submissions to Council should be clear and concise in terms of –

- recommendations
- the context in which these should be considered
- options and the implications of adopting these, including financial and other impacts, and associated risks
- rationale for resolutions sought
- implementation of strategies and responsibilities

See appendix 2 for the format in which papers to Council should be prepared.

7.2 **Timeframe**

Lengthy or complex papers to Council should be prepared in time for circulation to Councillors with the Council meeting business papers one week prior to the meeting date.

7.3 **Form**

A memo to Council should be in the approved form set out in this Handbook (see Appendix 2).

7.4 **Reporting responsibilities**

Each committee is to report monthly to Council.

8. IT Security and Privacy Policy

In connection with your role as a member of one or more of the Law Society of New South Wales' Committees you have been and will continue to be given access to IT services by the Law Society. The Law Society's IT Security and Privacy Policy includes provision for the mandatory data breach notification scheme under the *Privacy Act 1988* (Cth). The Policy includes a new Data Breach Response Plan.

The Law Society has determined that it is appropriate for the Policy to apply to Committee Members, who fall within the definition of "worker" in the *Work Health and Safety Act 2011* (NSW). "Workers" are in turn included in the Policy's definition of Law Society "Staff Member". Committee Members should read and familiarise themselves with the Policy generally, which is attached at Appendix 5, and in particular the Data Breach Response Plan.

6. RESPONSIBILITIES OF COMMITTEE CHAIRS

The Chairs of the committees are accountable to the Council for the output of those committees. It is the responsibility of the Chair to work with committee staff in relation to procedures to assist the efficiency and productivity of the committee. These should include the following:

1. Time commitment

1.1 Chairs must be prepared to commit a minimum of 10 hours per month for each committee and advise the President of the need for a replacement if they are unable to meet this commitment.

1.2 Management of The Law Society of New South Wales will arrange an induction/training session to be attended by all Chairs in January each year, session topics to include the conduct of meetings, monitoring of performance, relevant procedures and the Committee's advisory role to the President of The Law Society of New South Wales.

2. Annual directive

2.1 The committee's annual directive should comprise viable objectives, the achievement of which is capable of measurement.

2.2 The committee's program for the year comprises the means via which it meets those objectives and includes tasks determined by Council.

2.3 This combined document is to be settled by the staff officer with the committee Chair in consultation with the President if necessary and submitted to the Council for approval as part of its directives to committees.

3. Measures of performance

3.1 The committee Chair and responsible staff officer are responsible for monitoring the committee's achievements – such as completion of timetabled tasks, development and progress of committee agenda, and implementation of objectives.

3.2 Measures for assessing the performance of committee members include meeting set deadlines, record of attendance at meetings and general contribution to the work of the committee.

3.3 The President of The Law Society of New South Wales' approval can be sought to replace a committee member who is regularly unable to attend meetings and/or complete allocated tasks.

4. Meeting procedures

4.1 Commence meetings promptly at the scheduled times.

4.2 Allow committee members' views to be heard to the fullest extent possible.

4.3 Give clear directions to the responsible staff officer in relation to resolutions adopted.

7. RESPONSIBILITIES OF COMMITTEE MEMBERS

It is the responsibility of Committee appointees:

1. to inform themselves fully of the committee's mission/objectives, its tasks and agenda issues;
2. to be in a position to devote approximately one day per month to the work of each of their committees;
3. to attend meetings regularly or, if absence from a meeting is unavoidable, to inform the responsible staff officer in advance of their inability to attend;
4. to come to meetings well prepared with respect to agenda issues;
5. to participate fully in decision making on the direction the submissions and work of the committee will take, through the expression of their considered views on the matter being discussed; and by exercising where relevant the right of all individual members to cast his or her vote on those matters put to the vote in committee;
6. to inform the Chair of a conflict of interest or potential conflict of interest that may occur where personal interests or those of the appointee's firm could affect or be seen to affect the appointee's recommendations or decisions;
7. to undertake tasks requested by the Chair and/or the responsible staff officer, especially - although not exclusively - in areas in which the member has particular expertise, and to meet the agreed deadlines for completion of those tasks. From time to time members are asked to prepare submissions and comments at short notice;
8. to offer his or her resignation from the committee should he or she be consistently unable to meet these responsibilities due to work or other commitments. (Members who are absent for three meetings or more without a leave of absence may be invited to resign.)

8. RESPONSIBILITIES OF STAFF OFFICERS

1. Committee administration personnel

1.1 The staff member responsible for the work of a committee may be either a solicitor or a non-solicitor with other relevant experience.

2. Responsibilities

2.1 The responsibilities of these personnel are -

- to perform secretariat duties for their committees;
- to raise issues for the committee's consideration;
- to undertake appropriate research;
- to prepare draft recommendations, proposals and submissions for the committee's consideration;
- to undertake other tasks as directed by the Chair.

3. Tasks

3.1 **Contributions to the committee's agenda**

- Keep abreast of developments of interest to the committee through, for example
  - liaison with staff of other committees, political staff and bureaucrats, relevant outside bodies and individuals;
  - perusal of material received by the Society;
  - current knowledge of Society policy issues;
  - research.
- Include relevant issues on the committee's agenda.

3.2 **Facilitating committee discussion and decision making**

- Provide a focus for committee discussions by
  - developing views on matters to be discussed;
  - preparing executive summaries of lengthy documents;
  - drawing to the committee's notice aspects of reports, etc which require particular attention;
  - drafting recommendations in the form considered appropriate (letters, reports, proposals, etc) where a Society response is required.

3.3 **Meeting arrangements**

- Establish meeting dates, times and venues for the new year and circulate schedules to all committee members as soon as practicable.

3.4 **Agendas and business papers**

- Develop agendas and prepare and assemble papers for each meeting
  - the extent of consultation with the committee Chair on this task is the choice of individual Chairs;
  - agendas must be manageable in terms of length.
- Dispatch agenda papers seven days prior to the meeting date
  - late dispatch of papers and tabling of papers are to be avoided where possible.

3.5 **Meeting outcomes**

- Take notes of the meetings: the essential content of the outcomes comprises agreed actions and brief background to these actions;
- Circulate outcomes with the papers for the next meeting.

3.6 **Circulation of agendas, business papers and minutes**

These are circulated to -

- the committee Chair and all committee members
- any other designated members of staff

3.7 **Action arising from meetings**

- Follow up action items with each committee member who agreed to take responsibility for a particular item.
- Take action for which the staff member is responsible, including preparation of memoranda to Council and other tasks allocated by the committee Chair.

3.8 **Memoranda to Council and submissions to outside bodies**

- Prepare memoranda and submissions in accordance with quality principles.
- Memoranda to Council are to be in the attached form (Appendix 2) and a separate memorandum is to be prepared for each topic.
- Give notice to the Executive Officer, Council of items proposed for inclusion on the Council agenda in accordance with the schedule of Council meeting dates and due dates for papers published on the intranet.

9. SUB-COMMITTEES: ROLE AND FUNCTIONS

Set out below is an overview of the role and functions of sub-committees convened from time to time by the Law Society's 18 policy and practice committees.

1. Purpose

1.1 Committees may utilise sub-committees in the way most appropriate for their individual work programs. Some committees choose to establish standing sub-committees which may be in operation for the whole year while others prefer a system of ad hoc sub-committees formed to execute specific tasks. Some committees do not require sub-committees for their particular activities.

2. Scope and number

2.1 The scope and number of sub-committees convened from time to time will be determined by the committee Chair and policy lawyer for the committee. New sub-committees may be convened in response to legislative or other reform initiatives from existing committee members.

2.2 The number and role of sub-committees should be reviewed by the Chair and the policy lawyer and discussed with the Director, Policy and Practice Department, The Law Society of New South Wales at the commencement of the committee recruitment period each year.

3. Role

3.1 Sub-committees are subsets of the committee and have no separate role or authority to act outside normal committee processes. The members of each sub-committee will perform their role as committee members as described in this Handbook and as set out in this section. This includes the functions, in relation to their particular sub-committee areas, as listed on page 9.

4. Sub-committee operation

4.1 Each sub-committee may determine, by agreement of its members, how it proposes to deal with its committee tasks depending on the particular task, the timeframe and the preference of sub-committee members. Options include holding meetings in person, in which case the policy lawyer can assist by arranging to book Law Society of New South Wales meeting rooms if required, or by teleconference or by email.

4.2 The policy lawyer should attend subcommittee meetings unless otherwise agreed by the policy lawyer and Chair.

4.3 Where meetings of a sub-committee occur in the absence of the policy lawyer the sub-committee will provide a short report of the meeting and its outcomes to the Chair and the policy lawyer as soon as practicable after the meeting.

5. Reporting

5.1 To allow the sub-committees to function effectively, it is necessary for each sub-committee to report regularly to the Chair on any ongoing actions, copying the policy lawyer. The Chair or policy lawyer will, if considered appropriate, circulate any written communications, including emails to the whole committee.

5.2 Each sub-committee must report to the committee at each committee meeting on any actions or developments since the last committee meeting.

6. Sub-committee chair/spokesperson

6.2 The Chair may appoint a sub-committee Chair or spokesperson on an annual basis or in relation to a particular issue or task. The sub-committee Chair or spokesperson should report verbally or in writing to the committee at each committee meeting.

7. Joint sub-committees

7.1 There may occasionally be a proposal to convene a joint sub-committee made up of members of two or more committees. These are dealt with on an ad hoc basis and would not normally be considered necessary, for example, to draft a joint submission, where it is more common for each committee to provide comments which are then included in the joint submission coordinated by the relevant policy lawyer.

7.2 Where a joint sub-committee is formed, each contributing committee should receive regular reports on any actions or developments. The policy lawyer assisting the sub-committee will be able to advise on this process. Any proposal for the appointment of a joint sub-committee Chair should be considered by the Chairs of the contributing committees with the advice of the policy lawyer.

8. Queries

8.1 Any questions about the scope or operation of sub-committees should be directed to the committee's policy lawyer.

APPENDIX 1

Reimbursement of costs for country based committee members

APPENDIX 1

Reimbursement of costs for country based committee members

Cost calculations

1. Country based committee members are able to claim reimbursement of expenses incurred in calendar year by travel as follows:
   - return road travel x 11 (the maximum number of meetings commonly scheduled annually for committees),

   or

   - refundable return economy air fares from the member's region x 11

   or

   - return train travel

   or

   - a combination of the above over the year
2. The road travel claim per meeting is calculated at the rate of 78 cents per kilometre, regardless of car type or engine size. Note: from 1 July 2015, the government no longer provided for separate rates based on the size of the engine.
3. The air fares should be the cheapest economy fares offered by either Qantas "flexi saver", Rex "RexBiz" or Virgin.
4. Additional assistance capped at $350 per night is offered in respect of accommodation costs subject to the following conditions:
   - the member is domiciled more than 150 km outside Sydney and has travelled by either car, rail or air to the committee meeting;
   - return car, rail or air travel is not available due to the late conclusion of the committee meeting;
   - the member advises the Executive Officer, Council as soon as possible if he/she is likely to claim assistance for accommodation during the year.
5. Teleconferencing or video conferencing (for example, in the case of Rural Issues Committee meetings) will be utilised where feasible.

Claiming reimbursement

6. Claims are to be submitted in the calendar year that travel took place, and claims are only to be submitted post meeting/s. Reimbursement for December meetings can be applied for in the first 3 months of the following year.
7. Claims can be made on either a per trip or a per annum basis.
8. Claims are to be forwarded to the Executive Officer, Council and must state the name of the committee and the dates of the meetings against which travel assistance is being claimed.
9. For road travel claims, no additional information is required.
10. For air travel and accommodation claims, tax invoices must be provided with each claim to allow the Law Society to claim input tax credits, together with receipts where necessary to validate claims made. Practitioners may either
    - submit a bill as individuals to the Law Society (if the practitioner has personally incurred the air fare)

    or

    - submit the firm's tax invoice (if the travel costs are incurred by a firm).
11. Receipts or tickets are to be provided with claims for travel by taxi (e.g. to and from the airport) or by train and for parking.

APPENDIX 2

Memorandum to council

APPENDIX 2

Memorandum to council

TOPIC: ##

FROM: (Committee/Task Force/Other)

DATE: ##

Objective(s) and time limits
(eg to inform government of the Law Society's position on the proposed ... legislation; or to seek amendment of the Legal Profession Act 2004 for the purposes of ...; by ##[date])

Resolution(s) sought

A. RESOLVED that …….
1. ….

B. FURTHER RESOLVED that ….
C. NOTED that….

(OR, if a paper is for noting only, please use the following:

Resolution(s) Sought
Nil - For noting [and comments/feedback from Councillors])

Background

Existing Society policy
(eg international practice guidelines adopted by Council on ##[date])

Associated policy areas
(eg Aboriginal justice, consumer rights)

Overview/summary of issues
(outline main issues in point form)

Financial implications
(funding source for programs/activities: viz membership or licensing fees, or Public Purpose Fund

Confidentiality
(recommended level of confidentiality: full / partial / confidentiality not required)

Risk assessment
(Risks associated with recommended position/action and options.)

Public Relations Implications/PR Action Required
[Implications: eg nil / positive / negative for image of Law Society / profession]
[Action: eg to promote via media release / volunteer no public comment / prepare briefing paper]

Attachments

Person responsible for action required to execute resolution

Inclusion in LSJ Law Society of NSW Journal or enewsletter
(Yes/no)

(Signature)
(Responsible Policy Lawyer/Administrative Officer for ... Committee)

APPENDIX 3

Appropriate Workplace Behaviour Policy

Appropriate Workplace Behaviour Policy

Policy Principles

The Law Society of New South Wales strives to attract and retain the most qualified employees by taking steps to:

- provide equal opportunities with respect to compensation, benefits, promotions, development and other employment conditions; and
- promote a safe, healthy, inclusive and productive working environment for all employees.

The Law Society of New South Wales requires and expects all members of staff, whatever their level of responsibility, to maintain acceptable standards of workplace behaviour at all times, including treating everyone with respect, courtesy and inclusivity, and respecting diversity.

The Law Society of New South Wales is committed to creating a work environment where staff are treated with respect regardless of their personal characteristics, and which is free from unlawful discrimination, harassment and bullying, as part of providing a safe and healthy workplace.

Unlawful discrimination, vilification, harassment (including sexual harassment and sex based harassment), bullying and victimisation are unacceptable and will not be tolerated by the Law Society of New South Wales.

The Law Society of New South Wales recognises that employees should work in an environment that is free from unlawful discrimination, harassment and bullying and expressly prohibits any unlawful conduct, as outlined in this Policy.

Scope

Who does the Policy apply to?

This Policy applies to all employees (permanent, casual and temporary), volunteers, agents and contractors of the Law Society of New South Wales, collectively referred to in this Policy as 'workplace participants'.

Where and when does the Policy apply?

This Policy applies to the behaviour of workplace participants in the workplace and extends beyond The Law Society of New South Wales' premises and outside normal working hours, including:

- in the workplace, while working from home;
- public/common areas such as lifts and foyers;
- while undertaking work activities at other workplaces such as supplier or client premises;
- while using the Law Society of New South Wales' systems;

- outside of work hours if the interaction involves other workplace participants or members, including through social media;
- work-related travel; and
- work-related functions, for example lunches, conferences, Christmas parties, after-work drinks and client events.

Inappropriate behaviour may occur in internal and external communication of different types, including:

- verbal communication in person or over the phone;
- written communication such as letters, notes and faxes; and
- electronic communication such as email, text or instant messages and on-line social media/networking forums: Facebook, LinkedIn, Twitter etc.

This Policy applies to all areas of employment, including recruitment, terms and conditions of employment, promotion, transfer, training, leave and termination of employment. Workplace participants must also not engage in any unlawful conduct in the course of providing services to clients of the Law Society of New South Wales.

What type of behaviour is inappropriate?

Under State and Federal legislation and this Policy, the following types of conduct are unlawful and strictly prohibited:

- unlawful discrimination
- vilification
- workplace harassment
- bullying
- sexual harassment
- sex based harassment
- victimisation.

It is important to note that in some circumstances, workplace participants can be individually sued for their inappropriate workplace behaviour. Workplace participants who aid, abet or encourage other persons to engage in unlawful conduct can also be personally liable. In circumstances where a workplace participant's behaviour may involve a breach of the criminal law, the Law Society of New South Wales may also be obliged to notify the police or other relevant government authority.

You will be personally liable for your own actions if you engage in unlawful discrimination or unlawful harassment. An employer may be required to share liability for an employee's actions because of the legal principle relating to vicarious liability, although generally not where the employer has made the employee aware of their own obligations.

Discrimination

Unlawful discrimination occurs when a person is treated less favourably in their employment or a disadvantage is sustained because they have a certain attribute that is protected by law. Unlawful discrimination generally arises from stereotypes or assumptions about a person who has that attribute. There are a number of protected attributes under Federal and NSW laws (such as the *Age Discrimination Act* 2004 (Cth), *Disability Discrimination Act* 1992 (Cth), *Racial Discrimination Act* 1975 (Cth), the *Sex Discrimination Act* 1984 (Cth) and the *Anti-Discrimination Act 1977*

(NSW)).

Protected grounds include the following:

- sex
- age
- marital/domestic/relationship status
- religious belief or activity
- HIV/AIDS
- Carer/family responsibilities
- political belief or activity
- sexual orientation/preference, gender identity, gender expression, transgender status and intersex status
- pregnancy (including potential pregnancy) and breastfeeding
- disability or impairment, including physical, mental and intellectual disability
- race (including colour, nationality, descent, ethnicity, ethno-religious origin or national or social origin)

Unlawful discrimination may arise whether the person has the attribute now or had it previously, or where they are presumed to have it.

Unlawful discrimination may occur through:

- direct discrimination – where someone is treated less favourably because of their sex, age, race etc. For example, when an employee misses out on an internalpromotion because they are considered too old for the job; or
- indirect discrimination - where there is a rule, condition, requirement or practice which is on the same terms for everyone, but in fact is less favourable to / disadvantages someone with a protected attribute, and the condition, requirement or practice is unreasonable.

A person can unlawfully discriminate against another even if they did not intend to do so, if they treat that personless favourably because of one of these protected attributes.

Examples of Unlawful Discrimination

- failing to offer training to an older worker because you assume they will retire soon
- failing to give a female employee a promotion because she has children or is pregnant
- excluding a colleague from social functions because of their religion.

Vilification

Under Federal and NSW laws, vilification is a form of unlawful discrimination involving a public act which incites hatred, severe contempt or severe ridicule of a person or group on the basis of race, homosexuality, transgender, transsexuality or HIV/AIDS. A public act can include communication to the public in the media or on the internet through Facebook or Twitter. Serious vilification threatening or inciting physical harm to a person or group because they possess one of these characteristics is an offence under NSW laws and will be dealt with accordingly by the Law Society of New South Wales.

Harassment

Harassment is a form of unlawful discrimination. It is any form of behaviour that:

- is unwelcome or uninvited conduct;
- that a reasonable person would have anticipated would humiliate, offend, or intimidate the person exposed to the conduct; and
- is because of one of the protected characteristics above.

For example, harassing someone by making an insulting joke or derogatory remark about their race, age, religion, sexual orientation, disability etc is less favourable treatment of them than someone who does not have that characteristic and therefore constitutes discriminatory treatment.

Harassment does not have to be directed at a particular individual to be unlawful. Behaviour which creates a hostile working environment for other workplace participants can also be unlawful. The fact that no offence was intended, or that the behaviour was in jest, is not a defence.

Examples of workplace harassment

- racial or culturally insensitive jokes or nicknames
- derogatory remarks about a person's religion
- offensive comments about a person's sexuality
- teasing a person about their disability
- verbal abuse or comments that put down or stereotype people, jokes or offensive gestures, ignoring or isolating a person or group because of or based on any ground of discrimination
- mimicking someone's accent, or the habits of someone with a disability
- display or circulation of racist, pornographic or other offensive images or materials in any format
- sexual harassment (see below).

Sexual Harassment

Sexual harassment is unwelcome, unwanted or uninvited conduct of a sexual nature (including an unwelcome sexual advance or unwelcome request for sexual favours) in circumstances in which a reasonable person, having regard to all the circumstances, would have anticipated the possibility that the person exposed to the conduct would be offended, humiliated or intimidated.

Behaviour can amount to sexual harassment even if the person did not intend to offend, for example, because they were telling a joke. However, conduct will not be sexual harassment if a reasonable person would not have anticipated the possibility the conduct would offend, humiliate or intimidate theother person.
Sexual harassment is not behaviour which is based on mutual attraction, flirtation or friendship. If the behaviour is consensual and reciprocated, it is not sexual harassment. However, you should take great care before engaging in conduct you believe to be welcome and remember that some people may not feel comfortable telling you that your behaviour is offending them and is not welcome.

Examples of Sexual Harassment

Physical

- intimate physical contact, such as pinching, touching, grabbing, kissing or hugging
- sexual assault
- unnecessary familiarity - for example, deliberately brushing against a person
- unwanted physical contact - for example, touching or fondling.

Non-Physical

- staring or leering at a person or at parts of their body
- persistent requests to go out where they are refused
- suggestive comments about a person's body or appearance
- sexual jokes or comments/innuendo
- sexually explicit conversations or gestures
- displays of material containing nudity/semi-nudity or otherwise of a sexual nature such as posters, photographs, postcards, screen savers etc.
- viewing, accessing, downloading or transmitting nude/semi-nude, sexually explicit, pornographic or other material of a sexual nature using the internet or social media
- sending sexually suggestive or explicit emails, attachments or text messages
- offensive phone calls
- sexually explicit gifts e.g. 'Kris Kringle' gifts.

Both men and women can experience sexual harassment at work. Same-sex harassment is also covered. Often sexual harassment involves a pattern of unwelcome behaviour. However, one act is sufficient to constitute sexual harassment in some circumstances.

Sexual harassment does not have to be directed at a particular individual to be unlawful. Behaviour which creates a 'sexually hostile' working environment for other workplace participants can also be unlawful – for example, overhearing a colleague talking about sex, telling sexual jokes or making innuendoes.

It is important to understand that some forms of sexual harassment are also criminal behaviour and may be treated as a criminal offence. These include:

- sexual assault;
- physically molesting a person;
- indecent exposure; and
- obscene phone calls or emails/letters.

In some circumstances, workplace participants can be individually liable for their behaviour and comments and ordered to pay damages.

Sex Based Harassment

Sex based harassment is a particular form of harassment which the law does not allow. This occurs where:

- by reason of the sex of the person harassed (or a characteristic that relates to their sex or that is generally imputed to their sex);
- a person engages in unwelcome conduct of a seriously demeaning nature in relation to the person harassed; and
- in circumstances where a reasonable person, having regard to all the circumstances, would have anticipated the possibility that the person harassed would be offended, humiliated or intimidated.

Unlawful harassment on the ground of sex may occur alongside other forms of discriminatory conduct, including sexual harassment. The fundamental difference between sexual harassment and sex based harassment is whether the unlawful harassment is of a "sexual" nature. Sex based harassment includes conduct that is "seriously demeaning", but not necessarily "sexual".

Examples of sex based harassment may include but are not limited to:

- asking intrusive personal questions based on a person's sex, including in relation to their body, anatomy, sex or gender identity;
- making inappropriate comments and jokes to a person based on their sex (e.g. jokes about a gender stereotype or a gender specific condition like menopause);
- displaying or circulating images or materials (in any format) that are sexist, misogynistic or misandristic;
- making sexist, misogynistic or misandrist remarks about a specific person; or
- requesting a person to engage in degrading conduct based on their sex (e.g. intentionally making a mess and, in a seriously demeaning manner, asking a female to clean it up because of a gender stereotype).

Bullying

Bullying is repeated, unreasonable behaviour directed towards an individual or group that creates a risk to health and safety (physical or psychological). Unreasonable behaviour means behaviour that a reasonable person, having regard to all the circumstances, would expect to victimise, humiliate, intimidate or threaten another in the workplace. Bullying may be perpetrated by a colleague(s), a manager or even a client. It includes behaviour that degrades or undermines others in the workplace.

Bullying behaviour may also be unlawful discrimination, workplace harassment (based on a person's protected characteristic such as race,sex, age etc) and/or sexual harassment or sex based harassment. Or it may simply be based on personal dislike or animosity. A person canbe bullied for any reason. It can occur between a workplace participant and their manager, or between workplace participants.

For behaviour to constitute bullying it must be repeated (it can involve a range of behaviours over time). A one-off incident would not constitute bullying, although single incidents may still present a risk to health and safety. There is no requirement that the person deliberately or intentionally bully the person, however, intention may be relevant in assessing the severity of the conduct.

Examples of Bullying

- physical assault or threats
- abusive, insulting or offensive language or comments, or name calling

- teasing, humiliating comments or practical jokes
- deliberately excluding or isolating someone/ignoring them
- belittling opinions or unjustified criticism, particularly where communicated in front of others
- initiation rites
- deliberately withholding important information vital for effective work performance or denying access to supervision, consultation or resources to the detriment of the person
- intimidating actions
- rumours, gossip and innuendo
- encouraging other employees to participate in the bullying behaviour
- aggressive behaviour such as shouting/yelling, throwing objects or slamming doors
- allocating meaningless or impossible tasks to carry out
- intentionally setting unreasonable timelines or constantly changing deadlines
- intentionally setting tasks that are unreasonably below or beyond a person's skill level
- changing work arrangements, such as rosters and leave, to deliberately inconveniencea particular employee or employees.

Bullying can be carried out in a variety of ways, including through email or text messaging, internet chat rooms, instant messaging or other social media channels. It can be directed at a single employee or a group of employees and be carried out by one or more persons.

What is not Bullying?

Differences of opinion and robust debate are not bullying. Neither is interpersonal conflict, although conflict that is not resolved may escalate into bullying and should therefore be resolved wherever possible.

It is also not bullying for a Manager or Supervisor to take reasonable management action carried out lawfully, to counsel a workplace participant about their performance or conduct in a reasonable manner. Performance management and/or counselling are a necessary part of ensuring that workplace participants meet required standards of work and behaviour. While receiving negative feedback maybe stressful, it does not in itself constitute bullying. Provided they are carried out in a reasonable manner, other examples of reasonable management action include:

- transferring, demoting, counselling, warning, disciplining or dismissing an employee;
- setting performance goals, expectations and deadlines;
- refusing requests or making decisions not to provide a benefit;
- issuing work directions and orders;
- allocating work tasks consistent with business needs and systems;
- implementing organisational changes or restructuring;
- not selecting a person for promotion.

Bystander obligations

You must take action if you witness a workplace participant demonstrating unacceptable standards of workplace behaviour, including behaviour that amounts to unlawful discrimination, harassment, or bullying.

Ignoring the behaviour could be taken as tacit approval of the unacceptable workplace behaviour.

If a workplace participant is engaging in the unacceptable standards of workplace behaviour, where you feel comfortable, in the first instance you should encourage the other workplace participant to ask the person who is demonstrating unacceptable standards of workplace behaviour to stop and to make it clear that the behaviour is offensive, humiliating, intimidating, threatening, victimising, unreasonable, disrespectful or discourteous.

If this does not resolve the problem, you should encourage the workplace participant to make a complaint to their manager or supervisor or Human Resources, as soon as possible after the incident/s have occurred.

The by-stander could also bring the matter to the attention of their own direct manager or supervisor or Human Resources.

Although you may feel the need to tell a trusted friend or work colleague about the matter, you should treat the matter sensitively. Accusations of unacceptable standards of workplace behaviour can harm the reputation of those involved and could lead to legal action for defamation.

Victimisation

If a workplace participant feels they have been subjected to unlawful conduct, they are encouraged to raise the issue using the complaint procedure outlined in the Workplace Complaints Resolution Policy. It is unlawful to retaliate against or treat someone detrimentally because they have lodged a complaint, they intend to lodge a complaint or they are involved in a complaint of unlawful discrimination, harassment or bullying.

Workplace participants must not retaliate against a person who raises a complaint or subject them to any detriment. Doing so may result in disciplinary action up to and including termination of employment.

Further, the Law Society of New South Wales will not treat a workplace participant less favourably in their employment or engagement because they have made a complaint in good faith. However, if a person makes a false complaint in bad faith, that person may be disciplined, including termination of employment or contract.

Breach of this Policy

All workplace participants are expected to comply with the standards of behaviour contained in this Policy, as varied from time to time. A breach of a workplace participant's obligations under this Policy may result in disciplinary action, up to and including immediate termination of employment. In the case of agents or contractors, their contract may be terminated or not renewed.

If you observe someone else at work being subjected to behaviour that is potentially in breach of this Policy, the Law Society of New South Wales encourages you to report it.

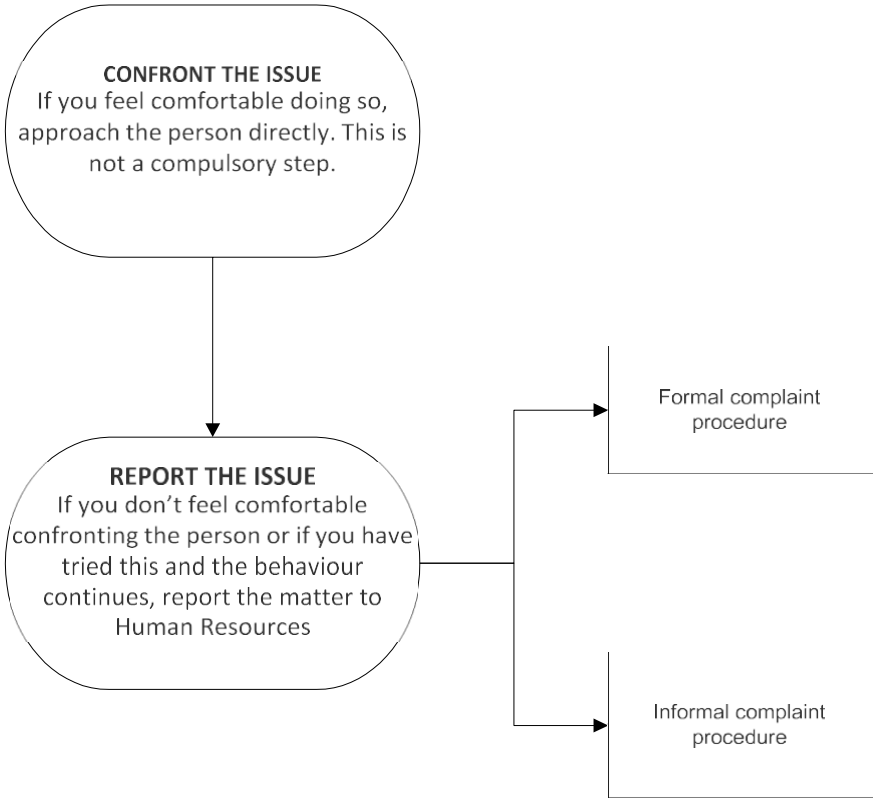
What should you do if you have a complaint?

If you feel that you have been subjected to any form of inappropriate behaviour in breach of this Policy, you should not ignore it (ignoring the behaviour could be taken as tacit approval of the behaviour).

As an initial step, if you feel comfortable doing so, address the issue with the person concerned. You should identify

the inappropriate behaviour, explain that the behaviour is unwelcome and offensive and ask that the behaviour stop. It may be that the person was not aware that their behaviour was unwelcome or caused offence. For example, you could say:

This is not a compulsory step. If you do not feel comfortable confronting the person, or you confront the person and the behaviour continues, you should report the issue under the Workplace Complaints Resolution Policy as soon as possible after the incident has occurred. The Law Society of New South Wales encourages all workplace participants to raise issues of conduct in breach of this Policy, and will treat all complaints seriously.



Workplace Participant Acknowledgement

You are required to review this Policy and keep yourself updated as to any changes that may be made to it from time to time. If you are unsure about any matter covered by this Policy, you should seek the assistance of your Manager or Human Resources.

This Policy does not form part of any contract between you and the Law Society of New South Wales. Any reference to obligations or requirements of the Law Society of New South Wales in this Policy does not, and is not intended to, give rise to contractual obligations binding on the Law Society of New South Wales.

External Resources

If at any time you have questions regarding this Policy, your obligations (including as abystander) or the complaint process, you are encouraged to contact Human Resources or your manager.

Staff and their immediate family members are able to obtain professional, confidential support by accessing the Law Society of NSW's Employee Assistance Programme. This is a confidential service and is not divulged to the Law Society of NSW. Details are available on the intranet or from Managers and the Human Resources Department.

You may also wish to seek counselling and assistance using Law Society of New South Wales' EmployeeAssistance Program (EAP) on:

EAP Australia (freecall):	1800 808 374

There are also a number of external organisations that may be able to offer assistance:

Lifeline	13 11 14
Beyond Blue	1300 224 636

The Law Society of NSW reserves the right to amend or replace this Policy at any time.

APPENDIX 4

Workplace Complaints Resolution Policy

Workplace Complaints Resolution Policy

Policy principles

The Law Society of New South Wales (the **Law Society**) aims to create and maintain a harmonious and productive work environment, free from conflict and inappropriate workplace behaviour. However, disagreements and grievances will arise in any workplace. Where the problem cannot be resolved between the parties involved, this Policy provides for a fair process to manage complaints.

The Law Society seeks to handle complaints in a confidential, impartial and timely manner, taking reasonable steps to prevent victimisation against those who raise a complaint in good faith (or assist someone else to do so).

Scope

This Policy applies to all employees (permanent, casual and temporary), volunteers, agents and contractors of the Law Society, collectively referred to as 'workplace participants'. Workplace participants can use this Policy to resolve a problem, concern or grievance (collectively referred to as a **Complaint**) during their employment or contract period that relates to work or the work environment. A Complaint may involve any of the following individuals:

- the Chief Executive Officer, senior manager, other manager, or other staff member;
- a Law Society Councillor or a member of a Law Society Committee;
- a contractor/consultant;
- a visitor to the workplace; or
- third parties dealt with in the course of performing work.

A complaint made by a former workplace participant about behaviour in the workplace, during that participant's engagement in the workplace, may be considered at the discretion of the Law Society, noting that the process outlined in this Policy may be modified or varied to take account of these circumstances.

A Complaint can be made about an act, omission, decision or behaviour that a workplace participant considers is unfair, unlawful or in breach of a policy of the Law Society, for example:

- acting up opportunities
- promotions
- transfers
- leave allocation
- work allocation
- hours of work, rosters or overtime
- work environment
- workplace health and safety
- discrimination
- harassment
- sexual harassment
- bullying

- training and development opportunities
- the nature of supervision
- performance appraisal

This Policy does not apply to complaints relating to the following:

- termination of employment, or termination or non-renewal of contract, of a workplace participant;
- improper conduct within the meaning of the Law Society's Whistleblower Policy; or
- complaints against staff made by Law Society members, other solicitors, or other non-workplace participants.

What should you do if you have a Complaint?

Workplace participants who have a Complaint should not ignore it. The Law Society encourages all workplace participants to raise issues under this Policy and will treat all Complaints seriously. Accordingly, once a Complaint is made, the Law Society will deal with the matter appropriately in accordance with this Policy.

Step 1 - Address directly with the person concerned

Where possible, parties involved in a Complaint are encouraged to attempt to resolve the Complaint between themselves, being closest to the source of the Complaint. As a first step, if a complainant feels comfortable doing so, he or she should address the issue with the person concerned. It may be that the person was not aware of the impact of their decision or behaviour. This does not mean that it is acceptable. However, it does mean that, in some circumstances, the issue can be resolved by simply advising the other person of the concern. They then have the chance to stop or to change what they have done or are doing.

This is not a compulsory step and should not be taken where it involves allegations of serious misconduct such as unlawful behaviour, serious forms of bullying or harassment or other serious abusive behaviours, or other conduct in the workplace that, if substantiated, is a serious risk to workplace health and safety.

Workplace participants are able to obtain professional, confidential support by accessing the Law Society's Employee Assistance Program. This is a confidential service and is not divulged to the Law Society. Details are available on the intranet or from the Human Resources Department.

Step 2 - Escalate to Contact Person

If directly addressing the problem does not work, or if the complainant does not feel comfortable with this approach or this approach is not appropriate in the particular circumstances of the Complaint, the Complaint may be escalated to the following persons (referred to as 'Contact Persons'):

- the complainant's manager;
- the complainant's manager's manager; or
- Human Resources Representative.

Where the Complaint involves a senior manager, a Councillor or a Committee member other potential Contact Persons can include the following:

- In the case of a senior manager (a direct report to the Chief Executive Officer), the Chief Executive Officer;
- In the case of the Chief Executive Officer, the Law Society President; or
- In the case of a Councillor or a Committee member, the Law Society President.

There are some situations where a workplace participant may not want to take a Complaint to their manager (for example if the complaint is of a sexual nature and the manager is of the other sex, or the Complaint is about or directly involves the manager). If so, the complaint can be taken to an alternative Contact Person.

The Contact Person will seek the involvement/assistance of Human Resources in the determination of the resolution process to be followed and the conduct of that process as appropriate.

Step	**Process**
Discuss	The Contact Person will discuss the Complaint with the complainant (unless there are exceptional circumstances such as a genuine risk to the safety of any person that could ensue from disclosure). They will explain the relevant steps that can be taken to address the Complaint. The Contact Person will generally need to meet with the complainant to discuss the Complaint. A support person can attend the meeting. If the Complaint is anonymous the Contact Person should immediately proceed to the assessment stage. If it is possible to contact the complainant (for example, where they have submitted the Complaint using a pseudonym email address), the Contact Person may attempt to contact the complainant to seek further details of the complaint if necessary for consideration in the Assess step below.
Assess	The Contact Person, with appropriate advice and support, will assess the Complaint including the nature of the Complaint, what the complainant has said during the Discussion stage (unless it is anonymous or discussion is not appropriate), what information is already available to support the Complaint or can be quickly and readily obtained through preliminary inquiries without interviewing witnesses or other more in depth investigation, whether any immediate action is required to ensure the safety of the complainant or any other workplace participant whilst the Complaint is being resolved (such as placing a person against whom a Complaint is made

	on leave, or temporarily redeploying a complainant). A Complaint must contain sufficient information to form a reasonable basis for further investigation. Mere allegation, without some verifiable information to support the allegation, will generally be insufficient to progress a complaint beyond the Assessment stage. Particular care should be taken in assessing whether to progress an anonymous complaint, that does not contain information capable of independent verification, in the absence of the ability to interview a complainant. The subject of the Complaint may be able to provide information useful in assessing a Complaint. There may be exceptional circumstances where this is not appropriate, for example, where there are likely to be serious health or safety consequences for an individual.
Determine Resolution Process	The Contact Person will then determine whether further action is warranted and, if so, the best way to deal with the Complaint. There are two types of Complaint procedures that can be used: informal and formal. The type of Complaint procedure used will depend on the individual circumstances. Usually, the process will involve speaking with the person(s) against whom the Complaint is made to obtain their account of events. In some cases, there may be sufficient evidence to substantiate a Complaint without the need for a formal investigation in which case it may be appropriate to proceed directly to disciplinary action.

What happens under the informal Complaint procedure?

Under the informal Complaint procedure there are a broad range of options for addressing the Complaint. The procedure used to address the issue will depend on the individual circumstances of the case.

Possible options include:

- the Contact Person discussing the issue with the person against whom the Complaint is made; and/or
- the Contact Person facilitating a meeting between the parties in an attempt to resolve the Complaint and move forward.

The informal Complaint procedure is generally suited to less serious Complaints that are unlikely to warrant disciplinary action being taken. In the informal Complaint procedure, there is no decision made about what did or

did not occur, but rather, the Contact Person attempts to facilitate an outcome that is acceptable to all parties, including the Law Society.

What happens under the formal Complaint procedure?

The formal Complaint procedure generally involves a formal investigation of the Complaint unless there are no disputed allegations. Formal investigations may be conducted by a member of staff considered suitable to conduct the investigation, or a person from outside the Law Society (including legal advisors or external investigators) appointed by the Law Society.

Where a Complaint involves a disputed allegation that, if substantiated (proven), may result in disciplinary action, it will generally be dealt with in accordance with the formal Complaint procedure.

An investigation involves collecting information about the Complaint and then making a finding based on the available information as to whether it is more likely than not that the alleged behaviour occurred or did not occur. Once a finding is made, the Law Society will consider any outcomes arising from the investigation.

If the Law Society considers it appropriate for the safe and efficient conduct of an investigation, workplace participants may be required not to report for work during an investigation. The Law Society may also provide alternative duties or work during an investigation. Employees will be paid their normal pay during any such period.

Disciplinary action or breach of contract action may proceed without formal investigation where there is no disputed allegation, for example the person, the subject of the Complaint, admits the conduct complained of.

Are Complaints confidential?

The Contact Person will maintain confidentiality as far as possible and therefore endeavour, as far as practicable, to limit disclosure of information about the Complaint to those who need to know. However, it may be necessary to disclose aspects of the Complaint in order to properly investigate or otherwise resolve the issue – for example, speaking with witnesses to determine what happened; to afford procedural fairness to those against whom the Complaint has been made; and to senior management/external advisors. Where criminal conduct is involved the Law Society may need to notify appropriate authorities.

If a Complaint raises matters which if proven would constitute a breach of the law or policies of the Law Society, appropriate action in relation to the Complaint will be taken (including completing the Complaint handling process), irrespective of the wishes of the complainant or others.

All workplace participants who are in any way involved in a Complaint procedure must maintain confidentiality, including the complainant. This includes what the Complaint is about and the identity of those involved. If a workplace participant breaches confidentiality, they may be subject to disciplinary action. Spreading rumours or gossip may also expose workplace participants to a defamation claim.

Workplace participants may discuss the Complaint with a designated support person or representative. However, the support person or representative must also maintain confidentiality.

Can I make my Complaint anonymously?

There are challenges in investigating anonymous Complaints whilst ensuring fairness to the person the subject of the Complaint. For an anonymous Complaint to be investigated, it must contain sufficient information to form a reasonable basis for investigation. Fairness to those subject to Complaints requires the avoidance of "fishing expeditions". Mere allegation, without provision of some substantial independently verifiable information to support the allegation, will generally be insufficient to progress an anonymous Complaint beyond the assessment stage.

How long does the Complaint process take?

Given the nature of Complaints and the need to maintain flexibility to resolve them, there is no set time frame for the Complaints process. The Contact Person will commence the Complaint handling process as soon as possible after a Complaint has been reported. The Complaint will be treated as a matter of priority in order to bring about a resolution as quickly as possible in the interests of all parties, and in fairness to the person complained of.

What if a Complaint has been made against me?

The Law Society seeks to handle Complaints in accordance with the principle of impartiality by giving both sides an opportunity to provide their account of disputed events.

Workplace participants who have had a Complaint raised against them are able to obtain professional, confidential support by accessing the Law Society's Employee Assistance Program. This is a confidential service and is not divulged to the Law Society. Details are available on the Intranet or can be obtained from Human Resources.

Possible Outcomes

The possible outcomes will depend on the nature of the Complaint and the procedure followed to address the Complaint, and whether the Complaint is against an agent, volunteer, employee or contractor. The procedures outlined below are intended as a GUIDE ONLY to the possible outcomes which may be implemented. In every case, the actual outcomes and/or disciplinary procedure to be adopted will be a matter for the Law Society to determine, in consideration of the circumstances as a whole.

What are the possible disciplinary outcomes?

If a Complaint results in a substantiated (proven) finding that a person has engaged in unlawful conduct or breaches of policy, or the person complained of admits the relevant conduct, that person may be disciplined. The type and severity of disciplinary action will depend on the nature of the conduct/breaches and other relevant factors concerning the employment or engagement of the person. Disciplinary action may include:

- a formal warning
- counselling

- transfer to another area
- suspension / termination of employment/ termination of contract

The Performance Management and Disciplinary Action Policy may apply to any admitted or substantiated (proven) findings of unsatisfactory behaviour or unsatisfactory conduct within the scope of that Policy involving an employee.

Where there is an admission or finding that an employee has engaged in serious or wilful misconduct, depending on the nature of the misconduct this may result in immediate dismissal.

Agents and contractors who are found to have engaged in unlawful conduct and/or breach of policy, or otherwise have breached their contracts, may have their contracts with the Law Society terminated or not renewed.

Any disciplinary action is a confidential matter between the affected workplace participant and the Law Society.

In the case of a Councillor or a member of a Law Society Committee, management of the outcome of a substantiated Complaint will be a matter for the Council in accordance with its Constitution and other legal and policy requirements.

Are there other non-disciplinary outcomes?

The Law Society may implement a range of other non-disciplinary outcomes to resolve a Complaint, depending on the particular circumstances. Examples include:

- training to assist in addressing the problems underpinning the complaint
- monitoring to ensure that there are no further problems
- requesting an apology
- requiring an undertaking that certain behaviour stop
- changing work arrangements.

What if the Complaint is not substantiated?

If a Complaint is not substantiated (i.e. there is insufficient proof of unlawful conduct or breach of policy), typically the following will occur:

- both parties will be informed that the Complaint could not be proven and, in general terms, the reasons why (for example, due to a lack of evidence);
- the standard of behaviour expected in the workplace will be explained to both parties;
- whether there is a need for generic intervention (e.g. training for all staff) will be considered;
- both parties will be warned about confidentiality and victimisation; and
- monitoring will occur.

The Law Society reserves the right to adopt a different approach, as appropriate in the circumstances.

Frivolous or vexatious complaints

Raising a Complaint under this Policy is a serious matter, with potentially serious consequences for those involved. If a person makes a false Complaint in bad faith (e.g. making up a Complaint to get someone else in trouble), that person may be disciplined, including termination of employment or contract. Such malicious Complaints can also expose the complainant to a defamation claim. Further, if a person lodges an excessive number of Complaints that the Law Society determines to be unfounded, they may be disciplined.

What to do if you are not satisfied with the outcome

Depending on the circumstances, the person may conduct the review by examining the paperwork only. They may decide that the original decision as to outcomes should remain, or that it should be overturned. The parties will be advised of the outcome of the review and the decision in relation to the review will be final.

Other Policies

This Policy should be read in conjunction with other policies and procedures of the Society including the:

- Professional and Personal Conduct policies;
- Appropriate Workplace Behaviour Policy;
- Whistleblower Policy;
- External Complaints Against Staff Resolution Policy
- Performance Management and Disciplinary Action Policy; and
- Law Society of New South Wales Privacy Policy.

Workplace Participant Acknowledgement

You are required to review this Policy and keep yourself updated as to any changes that may be made to it from time to time. If you are unsure about any matter covered by this Policy, you should seek the assistance of Human Resources.

This Policy does not form part of any contract between you and the Law Society. Any reference to obligations or requirements of the Law Society in this Policy does not, and is not intended to, give rise to contractual obligations binding on the Law Society. However disciplinary action including termination of employment or contract may be taken against any workplace participant who breaches this Policy.

The Law Society reserves the right to amend or replace this Policy at any time.

APPENDIX 5

IT Security and Privacy Policy

IT Security and Privacy Policy

Document Revision History

Version	Date	Changed By	Change Summary
1.0	13th Jan 2017	Lee Bustin	Initial Release
1.1	20th Feb 2017	Meaghan Lewis	Review and update
2.0	4th Aug 2017	Sophia Alifierakis	Review and update
3.0	8th Aug 2017	Sophia Alifierakis	BYO device provision
3.1	14th Sept 2017	Lee Bustin	BYO cleared up and made changes after CEO review
3.2	8th Oct	Lee Bustin / Meaghan Lewis / Sophia Alifierakis	Changes reflecting worker reference, councillors and YL distribution lists.
3.3	23rd Oct 2017	Lee Bustin	Final Version
3.4	23rd Feb 2018	Meaghan Lewis	Data Breach Response Policy
3.5	10th April 2020	Meaghan Lewis	Removal of Indemnity clauses under Annex. D
3.6	22nd October 2021	Marilyn Young	Reformatted policy to be in line with template guidelines
3.7	25 August 2022	Sarah Walters	Update staff details for Annexure G Data Breach Response Team

Distribution List

Name
For Councillors and Committees

TABLE OF CONTENTS

1. DOCUMENT OVERVIEW

Within this document, the Law Society of NSW will be referred to as "the Law Society".

The Law Society's directors and management are committed to conducting the Law Society's business ethically and in accordance with high standards of corporate governance.

It is important that this IT Security and Privacy Policy is clearly understood. We believe that good corporate governance practices assist to protect and enhance value within the business and encourages business best practice from all staff.

Our governance policies and procedures comply in all substantial respects with ITIL principles of good corporate governance and best practice recommendations. We will continue to review and, where necessary, to improve our governance practices to meet the Law Society's expectations.

This document has been developed to ensure all Staff Members of the Law Society understand their obligations and responsibilities with respect to IT Security and Privacy. The document MUST be read and understood by all Staff Members of the Law Society.

1.1 Code of Conduct

The Law Society acknowledges the need for directors, executives and Staff Members to observe the highest ethical standards of corporate behaviour. We have adopted a Code of Conduct to provide guidance on what is acceptable behaviour. Specifically, we require that all directors, managers and other Staff Members maintain the highest standards of integrity and honesty.

1.2 Applicability of Other Policies

This document is part of the Law Society's cohesive set of security and management policies. Other policies may apply to the topics covered in this document and as such, the applicable policies should be reviewed as needed.

1.3 Enforcement

This policy will be enforced by the Law Society's executive team. Violations of this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the Law Society will report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

2. ACCEPTABLE USE POLICY

2.1 Summary

(a) Overview

User network access is granted to Staff Members to enable them to perform their daily job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the IT network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation and thus the user is asked additionally to use common sense when using the Law Society resources. Questions on what constitutes acceptable use should be directed to the user's immediate manager.

(b) Purpose

Since inappropriate use of corporate systems exposes the Law Society to risk, this document specifies what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

(c) Scope

The scope of this policy includes any and all use of the Law Society's IT Network.

2.2 Detailed Policy

(a) E-Mail Use

Personal usage of the Law Society email systems is permitted as long as:

- Such usage does not negatively impact the corporate computer network; and
- Such usage does not negatively impact the user's job performance.

Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the Law Society may not be sent via email, regardless of the recipient, without proper encryption.

It is the Law Society's policy not to open email attachments from unknown senders, or when such attachments are unexpected or large in size.

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Users are expressly prohibited from modifying, removing or otherwise misusing, any of the following information from Law Society emails (or records of such emails):

- email header information;

- email signature blocks (i.e. so as to falsely impersonate another person); or
- the confidentiality/disclaimer terms inserted below a signature block.

(b) Confidentiality

Confidential data must not be:

- shared or disclosed in any manner to non-Staff Members of the Law Society;
- posted on the Internet or any publicly accessible systems; or
- transferred in any insecure manner.

Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

(c) Network Access

All Staff Members must take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access. Where a Staff Member discovers that they have access to areas of the network or information that is not directly related to their job function, this information must be reported to their direct management.

(d) Unacceptable Use

The following actions shall constitute unacceptable use of the IT network. The user may not use the IT network and/or systems to:

- engage in activity that is illegal under local, state, federal, or international law;
- engage in any activities that may cause embarrassment, loss of reputation, or other harm to the Law Society;
- engage in any commercial activity that is unconnected with the Law Society's commercial activities or purpose;
- disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media;
- download, install or use unauthorised software or programs;
- engage in activities that cause an invasion of privacy;
- engage in activities that cause disruption to the workplace environment or create a hostile workplace;
- view offensive websites (e.g. websites that are discriminatory);
- download or view pornographic or other objectionable material;
- engage in spamming or solicitations, send chain letters, or participate in pyramid schemes;
- impersonate another person;
- make fraudulent offers for products or services;
- perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of Staff Member's job function;
- install or distribute unlicensed or "pirated" software; or

- reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The Law Society may update or amend this list from time to time.

(e) Blogging

Blogging by the Law Society's Staff Members is subject to the terms of this policy, whether performed from the IT network or from personal systems. Blogging for personal use is never allowed from the corporate computer network. In no blog, including blogs published from personal or public systems, shall the Law Society be identified, the Law Society business matters discussed, or material detrimental to the Law Society published. The user must not identify himself or herself as a Staff Member of the Law Society in a blog. The user assumes all risks associated with blogging.

Acceptance to the above condition is given where blogging is being used for marketing or sales activity and is done with the express permission of senior management.

(f) Instant Messaging

Instant Messaging is allowed for corporate communications only. The user should recognise that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

(g) Overuse

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.

(h) Web Browsing

The Internet is a network of interconnected computers of which the Law Society has very little control. The Staff Member should recognise this when using the Internet and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The Law Society is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

The Law Society recognises that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of the Law Society IT Network should be in accordance with clause 2.2(o) below.

Users should be aware that all web browsing is subject to monitoring and recorded in accordance with the procedure set out in clause 2.2(l) below. Excessive web browsing, except for genuine Law-Society-related purposes, will be reported to senior management.

(i) Copyright Infringement

The Law Society's IT Network must not be used to download, upload, or otherwise handle illegal and/or unauthorised copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner:

- copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's;
- posting or plagiarising copyrighted material; or
- downloading copyrighted files which the employee has not already legally procured.

This list is not meant to be exhaustive; copyright law applies to a wide variety of works and applies to much more than is listed above.

(j) Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the IT network under any circumstance.

(k) Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only.

(l) Monitoring, Testing and Privacy

The Law Society advises that it undertakes ongoing monitoring, surveillance and security testing of its IT network, technical services and data usage. Surveillance occurs via software or other equipment that monitors the data input or output, or other use, of a device (including devices which are not owned by the Law Society (e.g. a Staff Member's personal mobile device)) used on the Law Society network or to access the Law Society technical services. Accordingly, users should expect no privacy when using the Law Society's IT network or technical services.

The information monitored by the Law Society may include but is not limited to:

- websites visited and cookies stored from those websites;
- emails sent and received using the Law Society's email server;
- files (whether uploaded, downloaded or stored);
- information posted on social network and blogging websites;
- messages and other data; and
- metadata from files opened and saved.

The Law Society reserves the right to monitor any and all parts of the IT network. This includes personal file directories and any mobile data devices (e.g. removable media such as USB drives).

In addition to ongoing monitoring and surveillance, the Law Society may also from time, and without notice, undertake certain testing exercises in respect of Staff Members' use of the Law Society computer network, for the purposes of assessing and improving the security of the network. An example of such a testing campaign is a "Phishing" exercise, whereby Staff Members' response to a (false) phishing email is assessed, and appropriate training is delivered in order to improve Staff Members' awareness and capabilities in this area.

(m) Notice of Monitoring and Surveillance

The Law Society will issue Notices to Staff Members advising of the monitoring and surveillance of its IT Network. Such Notices consist of:

- the Notice set out in **Annexure A** of this policy, which shall be distributed to all employees via email and posted in physical form in a prominent location in the Law Society's premises; and
- the Notice set out in **Annexure B** of this policy, which shall be displayed on all Law Society desktop computers upon start-up / boot.

The content and form of these Notices may be amended from time to time.

(n) Bandwidth Usage

Excessive use of the Law Society bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low the Law Society-wide usage.

(o) Personal Usage

Personal usage of the Law Society's IT Network is permitted during lunch, breaks, and before/after business hours, as long as such usage follows the relevant guidelines regarding usage elsewhere in this document and does not have a detrimental effect on the Law Society or on the user's job performance.

Users should be aware that all web browsing is subject to monitoring and recorded in accordance with the procedure set out in clause 2.2.(l) above. Excessive personal usage will be reported to senior management.

(p) Remote Desktop Access

Use of remote desktop software or services (such as Citrix, VNC, GoToMyPC, etc.) is prohibited, except where such software or services are approved and/or installed by the Law Society.

(q) Circumvention of Security

Using the Law Society's IT Network to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

(r) Use for Illegal Activities

The Law Society IT Network must not be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- unauthorised Port Scanning;
- unauthorised Network Hacking;
- unauthorised Packet Sniffing;
- unauthorised Packet Spoofing;

- unauthorised Denial of Service;
- unauthorised Wireless Hacking;
- any act that may be considered an attempt to gain unauthorised access to or escalate privileges on a computer or other electronic system;
- acts of terrorism;
- identity theft;
- spying;
- downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues; or
- downloading, storing, or distributing copyrighted material.

The Law Society will take all necessary steps to report and prosecute any violations of this policy.

(s) External Computer Equipment

The Law Society expressly prohibits the use of any external computer equipment on the Law Society's IT Network.

(t) Personal Storage Media

Personal storage devices represent a serious threat to data security and are expressly prohibited on the Law Society's network. All storage media must be supplied via the IT department any purchases by a Staff Member outside of this process will be deemed to be a personal purchase by that Staff Member regardless of whether the costs were recovered from the Law Society.

(u) Software Installation

Installation of any software or programs on the Law Society's IT Network which are not expressly approved and provided by the Law Society is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Further, software can cause conflicts or have a negative impact on the performance of the IT Network.

(v) Reporting of Security Incident

If a security incident or breach of any security policy is discovered or suspected, the user must immediately notify his or her immediate manager and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

- suspected compromise of login credentials (username, password, etc.);
- suspected virus/malware/Trojan infection;
- loss or theft of any device that contains the Law Society information;
- loss or theft of ID badge or keycard;
- any attempt by any person to obtain a user's password over the telephone or by email;
- any other suspicious event that may impact the Law Society's information security;

Users must treat a suspected security incident as confidential information and report the incident only to his or her manager or a member of the executive team. Users must not withhold information relating to a security incident or interfere with an investigation.

3. PASSWORD POLICY

3.1 Summary

(a) Overview

A solid password policy is an extremely important security control within the Law Society network. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy has been initiated by the Law Society to ensure industry best practice is adhered to.

(b) Purpose

The purpose of this policy is to specify guidelines for use of passwords. The policy will help users understand why strong passwords are necessary and help creation of passwords that are both secure and useable.

(c) Scope

This policy applies to any person who is provided an account on the Law Society's network or systems, including: Staff Members, guests, partners, vendors, etc.

3.2 Detailed Policy

(a) Construction

The Law Society follows a sound password construction strategy designed to ensure a high level of security. The organisation mandates that users adhere to the following guidelines on password construction:

- passwords should be at least 8 characters;
- passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols);
- passwords should be comprised of a mix of upper and lower-case characters;
- passwords should not be comprised of, or otherwise utilise, words that can be found in a dictionary;
- passwords should not be comprised of an obvious keyboard sequence (i.e., QWERTY); and
- passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Example: A way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

(b) Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the Law Society's proprietary information. The following guidelines apply to the confidentiality of the Law Society passwords:

- users must not disclose their passwords to any other person (co-workers, supervisors, family, etc.);
- users must not write down their passwords and leave them unsecured.;
- users must not login to the Law Society's IT Network using any other person's username or password, or attempt to do so;
- users must not check the "save password" box when authenticating to applications.;
- users must not use the same password for different systems and/or accounts;
- users must not send passwords via email; and
- users must not re-use passwords.

(c) Change Frequency

In order to maintain good security, passwords should be frequently changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. Users will be required to change passwords every 45 days. The Law Society will enforce this policy by expiring users' passwords after this time period.

(d) Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to their direct Manager. Any request for passwords over the phone or email, whether the request came from Law Society staff or not, should be immediately reported. When a user's password is suspected to have been compromised the user, or users, are required to immediately change their passwords.

4. GUEST ACCESS POLICY

4.1 Summary

(a) Overview

Guest access to the Law Society's IT Network is often necessary for customers, consultants, or vendors who are visiting the Law Society's offices. This can be simply in the form of outbound Internet access, or the guest may require access to specific resources on the Law Society's network. Guest access to the Law Society's network must be tightly controlled.

(b) Purpose

The Law Society may wish to provide guests with access to the IT network as a courtesy, or by necessity to visitors with a business need to access the Law Society's resources. This policy outlines the Law Society's procedures for securing guest access.

(c) Scope

The scope of this policy includes any visitor to the Law Society wishing to access the IT network or Internet through the Law Society's infrastructure, and covers both wired and wireless connections. This scope excludes guests accessing wireless broadband accounts directly through a cellular carrier or third party, where the traffic does not traverse the Law Society's network.

4.2 Detailed Policy

(a) Granting Guest Access

Guest access to the Law Society's IT Network will be provided on a case-by-case basis to any person who can demonstrate a reasonable business need to access the IT Network, or a reasonable business need to access the Internet via the Law Society IT Network.

(b) Guest - Acceptable Use and Computer Surveillance Notice

Guests must read, agree to and sign the Law Society's *Guest – Acceptable Use and Computer Surveillance Notice* as a precondition to being granted access to the Law Society's IT Network. A copy of the *Guest – Acceptable Use and Computer Surveillance Notice* is located at **Annexure C** of this policy.

(c) Approval

Guest need for access will be evaluated and provided on a case-by-case basis. This should involve management approval if the request is non-standard.

(d) Account Use

The Law Society may provide a generic guest account that can be re-used by different guests. If these accounts are offered, they are only to be used by guests. Users with network accounts must use their accounts for network access.

(e) Security of Guest Machines

Guests are expected to be responsible for maintaining the security of his or her machine, and to ensure that it is free of viruses, Trojans, malware, etc. The Law Society reserves the right to inspect the machine if a security problem is suspected, but will not inspect each guest's system prior to accessing the network.

(f) Guest Access Infrastructure Requirements

Best practices dictate that guest access is to be kept separate, either logically or physically, from the IT network, given that guests have typically not undergone the same amount of scrutiny as the Law Society's Staff Members. At a minimum, guest access must be logically separated from the Law Society's network via a demilitarised zone (DMZ), firewall, or other access controls. Guest access should be provided prudently and monitored for appropriateness of use.

(g) Restrictions on Guest Access

Guest access will be restricted to the minimum amount necessary. Depending on the guest needing access, this can often be limited to outbound Internet access only. The Law Society will evaluate the need of each guest and provide further access if there is a business need to do so.

(h) Monitoring and Privacy of Guest Access

Since guests are not Staff Members of the Law Society they are not considered trusted users. As such, the Law Society will monitor guest access to ensure that the Law Society's interests are protected and the Acceptable Use Policy is being adhered to. Accordingly, guests should expect no privacy when using the Law Society's network or IT Network.

The information monitored by the Law Society may include but is not limited to:

- websites visited and cookies stored from those websites;
- emails sent and received using the Law Society's email server;
- files (whether uploaded, downloaded or stored);
- information posted on social network and blogging websites;
- messages and other data;
- metadata from files opened and saved;

The Law Society reserves the right to monitor any and all parts of the computer network. This includes personal file directories and removable media.

5. DATA CLASSIFICATION POLICY

5.1 Summary

(a) Overview

Information assets are assets to the Law Society just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to the Law Society operations and the confidentiality of its contents. Once this has been determined, the Law Society can take steps to ensure that data is treated appropriately.

(b) Purpose

The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

(c) Scope

The scope of this policy covers all the Law Society data stored on the Law Society-owned, the Law Society-leased, and otherwise the Law Society-provided systems and media, regardless of location. Also covered by the policy are hardcopies of the Law Society data, such as printouts, faxes, notes, etc.

5.2 Detailed Policy

(a) Data Classification

Data residing on corporate systems must be continually evaluated and classified into the following categories:

- **Personal**: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply;
- **Public**: includes already-released marketing material, commonly known information, etc. There are no requirements for public information;
- **Operational**: includes data for basic business operations, communications with vendors, Staff Members, etc. (non-confidential). The majority of data will fall into this category;
- **Critical**: any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes;
- **Confidential**: any information deemed proprietary to the business. See the Treatment of Confidential Information Policy for more detailed information about how to handle confidential data.

(b) Data Storage

The following guidelines apply to storage of the different types of the Law Society data.

Personal:	There are no requirements for personal information.
Public:	There are no requirements for public information.
Operational:	Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.
Critical:	Critical data must be stored on a server that gets the most frequent backups (refer to the Data Backup Policy for additional information). System-level or disk-level redundancy is required.
Confidential:	Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or key card/keypad), with the key, keycard, or code secured.

(c) Data Transmission

The following guidelines apply to transmission of the different types of the Law Society data.

Personal:	There are no requirements for personal information;
Public:	There are no requirements for public information;
Operational:	No specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes;
Critical:	There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply;
Confidential:	Strong encryption must be used when transmitting confidential data, regardless of whether such transmission takes place inside or outside the Law Society's network. Confidential data must not be left on voicemail systems, either inside or outside the Law Society's network, or otherwise recorded.

(d) Data Destruction

The following guidelines apply to the destruction of the different types of the Law Society data.

Personal:	There are no requirements for personal information.
Public:	There are no requirements for public information.
Operational:	Cross-cut shredding is required for documents. Storage media should be appropriately sanitised/wiped or destroyed.
Critical:	There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.
Confidential:	Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

Paper/documents:	Cross cut shredding is required.
Storage media (CD's, DVD's):	Physical destruction is required.
Hard Drives/ Systems/ Mobile Storage Media:	Physical destruction is required. If physical destruction is not possible, the IT Manager must be notified.

6. TREATMENT OF CONFIDENTIAL INFORMATION POLICY

6.1 Summary

(a) Overview

Confidential data is typically the data that holds the most value to the Law Society. Often, confidential data is valuable to others as well, and thus can carry greater risk than general Law Society data. For these reasons the following security standards have been derived that relate specifically to dealing with confidential data belonging to both the Law Society and its business partners/customers.

(b) Purpose

The purpose of this policy is to detail how confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of confidential data and outlines specific security controls to protect this data.

(c) Scope

The scope of this policy covers all confidential data belonging to the Law Society, regardless of the location. Also covered by this policy are hardcopies of such confidential data, including printouts, faxes, file notes, etc.

6.2 Detailed Policy

(a) Treatment of Confidential Data

For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

(b) Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

(c) Transmission

Strong encryption must be used when transmitting confidential data, regardless of whether such transmission takes place inside or outside the Law Society's network. Confidential data must not be left on voicemail systems, either inside or outside the Law Society's network, or otherwise recorded.

(d) Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- paper/documents: cross cut shredding is required;
- storage media (CD's, DVD's): physical destruction is required;
- hard Drives/Systems/Mobile Storage Media: physical destruction is required. If physical destruction is not possible, the IT Manager must be notified.

(e) Use of Confidential Data

Proper adherence to the Law Society's Confidential Information Policy is dependent on users being aware of the Law Society's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- users must be advised of any confidential data to which they have been granted access. Such data must be marked or otherwise designated "confidential", "commercial in confidence" or "secret";
- users must only access confidential data to perform his/her job function;
- users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information;
- users must protect any confidential information to which they have been granted access and not reveal, disclose, release, share, email, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor;
- users must report any suspected misuse or unauthorised disclosure of confidential information immediately to his or her supervisor;
- if confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to the Law Society's outsourcing policy for additional guidance; and
- if confidential information is shared with a third party, the Law Society must indicate to the third party how the data should be used, secured, and, destroyed. Refer to the Law Society's Outsourcing Policy for additional guidance.

(f) Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. The Law Society requires that the following guidelines are followed:

- **Strong Encryption:** Strong encryption must be used for confidential data transmitted internally or externally to the Law Society. Confidential data must always be stored in encrypted form, whether such storage occurs on a user machine, server, laptop, or any other device that allows for data storage.
- **Network Segmentation:** The Law Society must use firewalls, access control lists, or other security controls to separate the confidential data from the rest of the IT network.
- **Authentication:** Two-factor authentication must be used for access to confidential data.

- **Physical Security:** Systems that contain confidential data, as well as confidential data in hardcopy form, should be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data.
- **Printing:** When printing confidential data, the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.
- **Faxing:** When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent: and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.
- **Emailing:** Confidential data must not be emailed inside or outside the Law Society without the use of strong encryption.
- **Mailing:** If confidential information is sent outside the Law Society, the user must use a service that requires a signature for receipt of that information. When sent inside the Law Society, confidential data must be transported in sealed security envelopes marked "confidential."
- **Discussion**: When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.
- Confidential data must be removed from documents unless its inclusion is absolutely necessary.
- Confidential data must never be stored on non-the Law Society-provided machines (i.e., home computers).
- If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

(g) Examples of Confidential Data

The following list is not intended to be exhaustive but should provide the Law Society with guidelines on what type of information is typically considered confidential. Confidential data can include:

- any Personal Information;
- employee or customer social security numbers, tax file numbers, or other personal information;
- medical and healthcare information;
- all Customer data, including financial records, all security and configuration related information regarding their infrastructures and systems, all staffing information, any other information regarding the customer that is not commonly known or understood but the Law Society is aware of due to the nature of our dealing with the customer;
- the Law Society's financial data;
- sales forecasts;
- product and/or service plans, details, and schematics;
- network diagrams and security configurations;
- communications about corporate legal matters;
- passwords;
- bank account information and routing numbers;
- payroll information;
- credit card information; or

- any confidential data held or understood for a third party (be sure to adhere to any confidential data agreement covering such information).

7. INCIDENT RESPONSE AND RISK MANAGEMENT POLICY

7.1 Summary

(a) Overview

A security incident can come in many forms and dependent upon the Law Society role/position actions taken may differ. A security incident can affect the Law Society or its members, customers or other stakeholders. The Incident Response Policy is critical to how successful recovery is from an incident. This policy covers all incidents that may affect the security and integrity of the Law Society's information assets and/or the information assets we manage on behalf of our customers. This policy is supplemented by the Data Breach Response Policy at section 10, which applies when an Eligible Data Breach concerning Personal Information is suspected or occurs.

Risk management or risk identification reduces the chances of an incident occurring.

This policy also outlines steps to take in the event of such an incident.

(b) Purpose

This policy is intended to ensure that the Law Society is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents.

Note: This policy is not intended to provide a substitute for legal advice, and approaches the topic from a security practices best practice perspective.

(c) Scope

The scope of this policy covers all information assets owned or provided by the Law Society, whether they reside on the IT network, customer's premises or elsewhere. To the extent that any security incident involves Personal Information, the Data Breach Response Policy at section 10 will apply.

7.2 Detailed Policy

(a) Types of Incidents

A security incident, as it relates to the Law Society's information assets, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

- **Electronic:** This type of incident can range from an attacker or user accessing the network for unauthorised/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection. It also includes the compromise of critical systems/infrastructures.
- **Physical:** A physical IT security incident involves the loss, damage, or theft of a laptop, network apparatus, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain the Law Society or its members', customers' or other stakeholders' information.

(b) Preparation

Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes having in place good systems, procedures and policy to:

- identify when an incident has or is going to occur;
- maintain good and proper audit trails should an incident occur to ensure a fast recovery from the incident and remediation or reprimand should this be required; and
- ensure that the damage that is done is minimised.

Additionally, prior to an incident, the Law Society must ensure that the following is clear to all Staff Members:

- What actions to take before, during and after an incident.
- Who is responsible to take which action.

(c) Risk Management Strategy

The following strategy should be adopted for identifying and dealing with risk:

- Identify the risk
  - What is the risk?
  - Where is the source?
  - What is the cause?
  - When does the risk occur?
- Analyse the risk
  - What are the consequences?
  - What is the rating of the risk?
  - What are the likelihood and potential outcomes?
- Evaluate the risk
  - Required treatments and options?
  - Costs to fix verse the risk to business?
  - Prioritise tasks?
- Treat risk
  - Allocate resources?
  - Fix required issues as per priorities?

- Monitor risk
  - Ensure the fix has resolved the problem?

(d) Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect the Law Society's and Staff Members' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the public regarding the Law Society or its members, customers and other stakeholders.

(e) Electronic Incidents

When an electronic incident is suspected, the Law Society's goal is to recover as quickly as possible, limit the damage done, secure the network or system, and preserve evidence of the incident. The following steps should be taken in order:

- Where applicable the compromised device should be isolated from the network. Do not power down the system.
- Immediately notify your direct manager and log a priority 1 ticket with the IT Team.

Note: If prosecution of the incident is appropriate, chain-of-custody and preservation of evidence are critical.

Following any electronic incident:

- The Law Society shall investigate and determine how the attack occurred and shall take appropriate steps to ensure this is remediated.
- Senior management shall notify applicable authorities if prosecution is appropriate and desired, based upon the evidence collected during the investigation.
- A review will be conducted (e.g. What can be learned? How did the Incident Response team perform? Was the policy adequate? What could be done differently?)
- A vulnerability assessment will be performed in an effort to identify any other vulnerability before they can be exploited.

(f) Physical Incidents

Physical incidents include but are not limited to:

- theft or loss;
- physical damage, intentional or unintentional; and
- physical compromise.

To ensure damage due to physical incidents are minimised the following actions must be adhered to:

- current backups of all configuration and system files must be kept. These include but are not limited to:
  - Firewalls: both the Law Society and managed customers.
  - Router and switches: both the Law Society and managed customers.
  - All other appliances: both the Law Society and managed not stated above.

- ensure all the Law Society and managed devices are under current vendor management and replacement contracts;
- all devices have been configured on the Law Society monitoring systems; and
- all devices have been listed on the Law Society asset register.

(g) Response

Establish the severity of the incident by determining the potential risk to the Law Society or to its members, customers or other stakeholders:

- *Was confidential data involved?*
  If yes, refer to the "treatment of confidential information policy".
- *Could the device be compromised?*
  If yes, refer to the "incident response and risk management policy".

If the incident was due to physical damage caused to the device determine how the damage occurred. Where damage is caused to the Law Society owned devices that reside at a Staff Member's premises and it is determined that the damage was not caused due to normal wear and tear and has been caused by that Staff Member, the responsibility for cost to replace the equipment remains with that Staff Member. Examples include but are not limited to:

- Device being dropped
- Device being overheated
- Water damage

(h) Incident Contained

- Ensure all information regarding the incident has been captured within IT Support Centre.
- Ensure any potentially compromised username, password, account information, WEP/WPA keys, passphrases, etc., which were stored on the system has been changed.
- Replace the lost hardware and restore data from the last backup.
- Notify the applicable authorities if a theft has occurred.
- Manager in control of incident must complete an incident response notification to all relevant persons involved or affected.
- Review procedures to ensure that risk of future incidents is reduced.

(i) Notification

If an electronic or physical security incident is suspected to have resulted in the loss of third-party or member, customer or other stakeholder data the executive team is responsible for formulating a response in accordance to these policies and State, Territory, and country regulations. If the third-party or member, customer or other stakeholder data comprises Personal Information, the matter should be dealt with in accordance with the Data Breach Response Policy at section 10.

8. PHYSICAL SECURITY OF INFORMATION TECHNOLOGY ASSETS

8.1 Summary

(a) Overview

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations, servers and network storage appliances and transmitted on the Law Society's physical network infrastructures. This can be both the Law Society information, and customer information. In order to secure the Law Society and customer information, thought must be given to the security of the Law Society's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

(b) Purpose

The purpose of this policy is to protect the Law Society's physical information systems by setting standards for secure operations.

(c) Scope

This policy applies to the physical security of the Law Society's information systems, including, but not limited to:

- All the Law Society-owned or the Law Society-provided network devices, servers, personal computers, mobile devices, and storage media.
- All the Law Society owned systems managed on behalf of our members, customers or other stakeholders.
- Additionally, any person working in or visiting the Law Society's office is covered by this policy.

Note: that this policy covers the physical security of the Law Society's Information Technology infrastructure, and does not cover the security of non-IT items.

8.2 Detailed Policy

(a) Locating Critical Systems

When possible, thought should be given to selecting a site for the housing of IT devices that is secure and free of unnecessary environmental challenges. At a minimum, the location where critical systems are stored should meet the following criteria:

- The location should be chosen where the equipment will not be susceptible to damage caused by water, heat or severe cold.
- The location should be secure to deter theft.
- Where possible environmental controls should be in place.
- Where possible entry points to the location should maintain access controls.

(b) Security Zones

The Law Society will maintain standard auditable security controls. These include but are not limited to:

- External monitored alarm systems.
- Zoned logged access restrictions utilising keycard technologies.
- Video monitoring to key areas.

(c) Access Controls

Access controls are necessary to restrict entry to the Law Society premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with the Law Society's guidelines for their use.

(d) Keycards

The Law Society requires that keycards be used for all user access controls. Key cards have an advantage over keys in that access policies can be tuned to the individual user. Schedules can be set to forbid off-hours access, or forbid users from accessing a security zone where they are not authorised. If a keycard is lost or stolen it can be immediately disabled. If a Staff Member is terminated or resigns, that user's access can be disabled.

- Staff Members are not permitted to give their keycards out under any circumstances.
- Staff Members must report their keycards lost immediately.
- Keycards are not to be left unattended in open view.

(e) Physical Data Security

Certain physical precautions must be taken to ensure the integrity of the Law Society and our members', customers' and other stakeholders' data. The following guidelines must be followed:

- Computer screens must be positioned where information on the screens cannot be seen by outsiders.
- Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorised to view the information.
- Users must log off or shut down their workstations when leaving for an extended time period, or at the end of the workday.
- Network cabling must not run through non-secured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).
- Remote access to the Law Society's network must be done over a secured connection.

(f) Physical System Security

In addition to protecting the data on the Law Society's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

(g) Minimising Risk of Loss and Theft

In order to minimise the risk of data loss through loss or theft of the Law Society property, the following guidelines must be followed:

Unused systems:	If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.
Mobile devices:	Special precautions must be taken to prevent loss or theft of mobile devices. Refer to the Law Society's Mobile Device Policy for guidance.
Systems that store confidential data:	Special precautions must be taken to prevent loss or theft of these systems.

(h) Minimising Risk of Damage to Hardware Systems

In order to minimise the risk of damage to hardware proper care must be taken when working with, transporting, mounting and storing these systems. It is important that the following guidelines are adhered to:

- Environmental controls should keep the operating environment of the Law Society systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimised.
- Strong magnets must not be used in proximity to the Law Society systems or media.
- Except in the case of a fire suppression system, open liquids must not be located above the Law Society systems. Technicians working on or near the Law Society systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto the Law Society systems.
- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for important systems and encouraged for all systems.
- Only those Staff Members whose role dictates are permitted to maintain the Law Society systems.

(i) Fire Prevention

It is a policy of the Law Society to provide a safe workplace that minimises the risk of fire. The guidelines below are intended to be specific to the Law Society's information technology assets and should conform to the Law Society's overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.
- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.

- Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
- Only approved electrical equipment must be used.
- Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) where possible.
- Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.
- A smoke alarm detection device - Alert a designated Law Society Staff Member if an alarm is tripped during non-business hours.

9. BYODs ("Bring Your Own Device(s)")

9.1 Summary

This policy covers the approval, usage and security controls in respect of the provision of Law Society Mobile Services on BYODs used by Staff Members.

This policy contains the requirements and processes that must be adhered to in respect of BYODs used by Staff Members.

For the requirements and processes that must be adhered to in respect of Law Society Mobile Devices used by Staff Members, Staff Members should refer to the separate IT Policy relating to Law Society Mobile Devices - Mobile Services and Mobile Plans.

9.2 Detailed Policy

(a) BYOD

BYOD(s) remain the property of the Staff Member at all times.

The Law Society's IT Department does not provide any formal handset support or assistance with configuration settings for any BYOD used by a Staff Member. The IT Department will provide a best endeavours support but you may need to engage with your network provider and handset manual to complete the setup or to obtain any such support in respect of the BYOD.

(b) BYOD and Personal Mobile Plan

Where a Staff Member uses a BYOD combined with a Personal Mobile Plan – the Staff Member should execute the attached "Deed relating to the use of Law Society Mobile Services on BYOD(s)" – see Annexure D.

- **Staff Member's Personal Mobile Plan**
  The use of a Personal Mobile Plan for Law Society business may be agreed with a Staff Member either on a permanent basis or an ad-hoc basis. If it is agreed with you that a Personal Mobile Plan should be used on a permanent basis, the assumption is that your role and duties require the use of a Mobile Plan on a

regular and ongoing basis. A Personal Mobile Plan agreed on an ad-hoc basis is more appropriate in a one-off situation such as for the purposes of attending a conference outside of the Law Society premises.

- **Personal Mobile Plan – Permanent**
  Staff Members who require a Mobile Plan for the purposes of performing their regular duties for the Law Society should do this via the Mobile Plan with their own mobile carrier. In this situation, the risk of incorrect and fraudulent charges and any supplier management issues with the carrier is the responsibility of the Staff Member and not the Law Society.

  The cost of a Staff Member's use of a Personal Mobile Plan in connection with Law Society business should not exceed the Law Society's own Corporate Mobile Plan costs.

  Any charges incurred in excess of this amount will not be the responsibility of the Law Society. Any request by a Staff Member for reimbursement for any excess amount should be made in writing to the Law Society CEO or COO.

  The Law Society reserves the right to remove this privilege and may choose only to offer Staff Members a Mobile Plan under the Law Society's Corporate Mobile Plan.

- **Personal Mobile Plan – Ad-hoc**
  Staff Members who do not require a Mobile Plan for the purposes of performing their regular duties for the Law Society may claim reimbursement from the Law Society for any work-related usage of their BYOD, where it can be demonstrated that the BYOD has been used for business purposes.

  Claims for reimbursement may be made by a Staff Member where a detailed bill for the relevant BYOD can be provided to the Law Society by the Staff Member. Any charges incurred in respect of Law Society business should be highlighted. Where a Staff Member's Personal Mobile Plan includes the cost of business calls and/or data, a maximum of 30% of the total monthly bill can be claimed from the Law Society by that Staff Member.

- **Personal Mobile Plan – SIM PIN**
  A SIM PIN is a four digit PIN and is only used when a device is turned on. The SIM PIN is separate to the locked screen PIN / access code. Use of a SIM PIN by Staff Members using a Personal Mobile Plan is highly recommended by the Law Society in order to prevent fraudulent charges (e.g. if a device is stolen). However, this is not compulsory. The Law Society's IT Department will provide and record the SIM PIN. Please contact the IT Department should you fail to remember your PIN or for more assistance (IT.Support@lawsociety.com.au).

(c) International Usage – Applies to All Mobile Plans

If you are travelling overseas for business, you should please contact the Law Society's IT Department (IT.Support@lawsociety.com.au) for a fact sheet on ways to minimise your spend on data and internet usage.

Any calls should be made via the Law Society's Skype service or other approved data call services (e.g. Apple FaceTime) which utilise the Wi-Fi network. Please contact the Law

Society's IT Department (IT.Support@lawsociety.com.au) for further details of recommended and approved applications.

All data roaming must be switched off at all times on your Mobile Device be it in Australia or overseas. Data roaming is not needed whilst in Australia so leaving it off will ensure it is not active when you travel overseas.

You are only permitted to download emails overseas when you have access to Wi-Fi (hotels, office, airports etc.). You are not permitted to switch on data roaming at any time to retrieve your emails whilst traveling.

You will be responsible for paying any data costs are incurred whilst overseas. Any exceptions to this policy should be made should be made in writing to the CEO or COO.

(d) Premium Mobile Plan Services

The Law Society will not be responsible for any premium mobile service costs incurred on a Personal Mobile Plan.

(e) Stolen Equipment (report within 24 hours)

Should your Mobile Device be lost or stolen, you must report the matter to IT and your Manager within 24 hours, whether the lost or stolen device is a Law Society Mobile Device or a Staff Member's own personal Mobile Device. This is to limit any unauthorised usage of the Mobile Plan and enable the Law Society to secure its business data.

The Law Society will not be responsible for any unauthorised costs incurred on a Personal Mobile Plan.

(f) Hands Free Operation

The use of any Mobile Device whilst driving is forbidden unless hands-free kits are fitted. It is an offence (driving without due care) to use a Mobile Device whilst operating a motor vehicle and the incursion of any fines or penalties will be the sole responsibility of the relevant Staff Member. Any vehicle damage incurred as a result of this practice, which is not recoverable through insurance, may be recovered by affected parties from a relevant Staff Member.

If you do not have a hands-free kit fitted, do not use your Mobile Device whilst driving. The Law Society will not accept any excuse for such use of a Mobile Device (including any argument that budget restrictions or non-use of particular equipment lead to an offence).

(g) On Leaving the Law Society

On resignation or termination of your employment or otherwise ceasing your engagement with the Law Society, you should remove all work-related data from any BYOD used for any Law Society business.

In addition, the IT Department will remove all work-related information (contacts, mail, calendar, files, etc.) from your own personal Mobile Device on resignation or termination of

your employment or other ceasing of your engagement with the Law Society. This may be conducted remotely and without notice by the IT Department on or after your leaving date.

If you have configured Law Society data or service e.g. work email on your personal device, you must contact the IT Department prior to leaving the Law Society to request the removal of the Law Society data settings. Failure to do so may result in loss of personal data.

10. Data Breach Response Policy

10.1 Summary

(a) Overview

This Data Breach Response Policy sets out the procedures that the General Counsel and the Data Breach Response Team (as defined in Annexure G) will follow to address data breach notification requirements and any other legal obligations that may apply in the event of an actual or reasonably suspected data breach.

(b) Purpose

The purpose of this policy is to comply with the notifiable data breaches scheme implemented under the *Privacy Act 1988* (Privacy Act), which requires the Law Society to notify any affected individuals and the Privacy Commissioner at the Office of the Australian Information Commissioner (OAIC) of any data breaches that are likely to result in serious harm to an affected individual (i.e. an individual whose Personal Information is involved in the breach). If the Law Society takes certain remedial steps to address a data breach, or other exceptions apply, the Law Society may not be required to notify.

(c) Scope

All Law Society Staff Members will follow this policy.

10.2 Detailed Policy

(a) Key Documents

This policy includes four Annexures that all Law Society Staff Members must adhere to:

- **Annexure E** identifies the procedures that all Law Society Staff Members must follow in the event of an actual or suspected data breach.
- **Annexure F** sets out an email template form for reporting any actual or suspected data breaches to the General Counsel.
- **Annexure G** lists the Data Breach Response Team's roles and responsibilities.

- **Annexure H** summarises in a flowchart the procedures to follow in the event of an actual or suspected data breach.

(b) Key Concepts

Eligible Data Breach

- involves unauthorised access to, disclosure of, or loss of, Personal Information held by the Law Society; and
- is likely to cause serious harm to the affected individuals, determined on an objective assessment from the viewpoint of a Reasonable Person in the Law Society's position (i.e. the Data Breach Response Team).

(c) Detection of a data breach

Any Law Society Staff Member who discovers, suspects or is notified about a data breach must immediately report such incident to the General Counsel of the Law Society and no other person (unless subsequently authorised by the General Counsel) so that the General Counsel can advise as to next steps.

The responsibilities of Law Society Staff Members are set out in **Annexure E**.

The General Counsel will raise an internal report regarding a known or suspected data breach with the Data Breach Response Team as soon as possible.

(d) Role of the Data Breach Response Team

The goal of the Data Breach Response Team is to collect information about the incident including about:

- the source of the data breach;
- the full impact of the data breach, including the data affected and whether it is under the control of, or has been accessed or copied by, an unauthorised person;
- who is aware of the data breach, both internally and externally;
- the risk of harm resulting from the data breach;
- whether the data affected by the data breach is Personal Information covered by breach notification requirements under the Privacy Act; and
- the appropriate action to be taken.

The key questions the Data Breach Response Team will focus on are:

- has there been unauthorised access to, or unauthorised disclosure of Personal Information, or a loss of Personal Information?

- is this likely to result in serious harm to one or more individuals?
- is the Law Society able to prevent the likely risk of serious harm?
- other relevant questions based on the circumstances, such as the value of the data or issues of reputational risk?

The Data Breach Response Team, with the General Counsel's assistance, will determine what state and federal laws apply to the data breach in question, and may advise whether the incident involves a breach of contract or undertaking to a third party, involves Personal Information and potentially gives rise to mandatory data breach notification obligations. The General Counsel may involve outside counsel as necessary to implement this policy.

(e) Actions following a suspected or actual data breach

If there are reasonable grounds to suspect there may have been a data breach, the Data Breach Response Team must:

- carry out an expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an Eligible Data Breach, in accordance with this Policy; and
- take all Reasonable Steps (including, without limitation, dedicating sufficient Law Society Staff Members to the assessment who have sufficient access to the relevant systems) to ensure that such assessment is carried out **within 30 days** of becoming aware of the reasonable grounds for suspicion.

In order for the assessment to be "reasonable and expeditious" the amount of time and effort expended must be proportionate to the likelihood of the breach and its apparent severity.

If the Data Breach Response Team cannot make the assessment within 30 days, the Data Breach Response Team will document why there is a delay and keep records to show:

- that the Law Society has taken all Reasonable Steps to complete the assessment within 30 days;
- the reasons for any delay; and
- that the Law Society's assessment was reasonable and expeditious.

Forensic Investigation
Before entering into any forensic investigation into the circumstances around an Eligible Data Breach, the Data Breach Response Team should consider whether the investigation is for the purpose of establishing its legal position. If so, the Law Society should consider retaining an external law firm in order to better support any future claim for legal professional privilege.

Actions
The 4 steps the Data Breach Response Team will follow when a data breach is discovered are:

1. contain the breach;

2. evaluate the risks associated with the breach;
3. notification, if applicable; and
4. prevention of future breaches.

(1) Containing the breach

In the event there is an actual data breach, the Data Breach Response Team will:

- take all necessary steps to immediately contain the impact of any data breach;

  For example, the Law Society may stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then the Law Society may consider revoking or changing computer access privileges or addressing weaknesses in physical or electronic security.

- assess whether steps can be taken to mitigate the harm an individual may suffer as a result of any breach.

  For example, if an individual's bank account details have been exposed, the Law Society may consider instructing the individual to contact their financial institution to put them on notice of any unauthorised activities.

The Law Society will carry out these steps with a view to:

- reducing the adverse impact of any data breach;
- preventing further expansion of any data breach; and
- preserving the affected data.

.

(2) Evaluating the risks associated with the breach

The Law Society must act reasonably in determining whether there is likely to be serious harm. Serious harm could include physical, psychological, emotional, financial or reputational harm.

The Data Breach Response Team will consider the following questions to determine whether there is likely to be serious harm - the answers will be considered in whole considering the likelihood or harm to individuals and the consequences of the harm:

The type of Personal Information involved

- Whose Personal Information was involved - any young persons, any vulnerable individuals?
- Does the type of Personal Information that has been compromised create a greater risk of harm? For example:
  - Is the harm physical, financial or psychological?
  - Has a combination of Personal Information been exposed?
  - Is the information permanent or temporary (i.e. cannot and can be reissued)?
- Who is affected by the breach? Employees, contractors, the public, service providers, Law Society members or other agencies/organisations?

- How many individuals were involved? (A larger number suggests a higher risk of serious harm)

The context of the affected information and the breach

- What is the context of the Personal Information involved (e.g. is the Personal Information sensitive)?
- Is the Personal Information related to an individual's finances, health, documents which are commonly used for identity fraud (e.g. Medicare card, driver's licence, passport details), or is it a combination of Personal Information?
- Would the information publicly associate an individual's Personal Information with a sensitive product or service?
- Have there been other breaches that could have a cumulative effect?
- How could the Personal Information be used?

The cause and extent of the breach

- Is there a risk of ongoing breaches or further exposure of the Personal Information?
- Is there evidence of threat? This could suggest a greater intention to do harm and heighten the need to provide notification to the individual as well as law enforcement.
- Is the Personal Information protected by one or more security measures e.g. it may have been encrypted, anonymised or otherwise not easily accessible)?
- How likely is it that one or more of those security measures were successful or failed? Was there appropriate industry standard security?
- If the Personal Information is encrypted, how likely is it that the persons who have obtained or could obtain the information, and have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates, are able to circumvent the encryption? Does the attacker have the encrypted data and the encryption key?
- What was the source of the breach? For example, was it external or internal malicious behaviour or was it an internal processing error? The risk of harm to the individual may be less where the breach is unintentional or accidental.
- Has the Personal Information been recovered?
- What steps have already been taken to mitigate the harm?
- Is this a systemic problem or an isolated incident?
- How many individuals are affected by the breach?

The risk of serious harm to the affected individuals

- Who are the persons, or the kinds of persons, who have obtained, or who could obtain, the Personal Information?
- Is there any relationship between the unauthorised recipients and the affected individuals?
- What harm to individuals could result from the breach? For example:
  - identity theft;
  - significant financial loss by the individual;
  - threat to an individual's physical safety;
  - threat to emotional wellbeing;
  - loss of business or employment opportunities;
  - humiliation, damage to reputation or relationships; or

- workplace or social bullying or marginalisation.

The risk of other harms

- Are there any other possible harms, including to the agency or organisation that suffered the breach? For example:
  - the loss of public trust in the Law Society;
  - reputational damage;
  - loss of assets (e.g. stolen computers or storage devices);
  - financial exposure (e.g. if bank account details are compromised);
  - regulatory penalties (e.g. for breaches of the Privacy Act);
  - extortion;
  - legal liability; and
  - breach of secrecy provisions in any applicable legislation.

(3) **Notification**

If a data breach creates a real risk of serious harm to the individual, the Law Society must notify affected individuals. The Data Breach Response Team will consider the advice from the General Counsel and determine:

- **Remediation:** whether, in the circumstances, any steps can or should be taken to remediate or mitigate the impact of the data breach and avoid any serious harm. If the Data Breach Response Team takes remedial action such that the Eligible Data Breach does not cause serious harm, the notification obligations will not apply.

- **Notice to Reporting Agencies:** whether it is necessary or appropriate to notify any relevant authorities (whether the Office of the Australian Information Commissioner or other authorities), or consumer reporting agencies and the nature of that notification. In particular, the Data Breach Response Team will consider whether authorities should be notified even if there is some doubt that a strictly notifiable data breach has occurred and in that case whether the form of advice to the authorities should constitute an application to the Australian Information Commissioner (i.e. the Privacy Commissioner) for an exemption from the obligation to notify individuals in the event that the Privacy Commissioner disagrees that the circumstances are not notifiable.

- **Notice to Individuals:** whether it is necessary or appropriate to notify affected individuals about the data breach. The Data Breach Response Team will also consider and determine whether to provide notice even if not legally required in light of other policies of the Law Society and its commitment to its members, customers and employees.

How to notify

- **Providing a statement to the Privacy Commissioner**
  Notification to the Privacy Commissioner should be carried out using the designated form accessible on the OAIC website:
  https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB
  and sending it to the Privacy Commissioner at enquiries@oaic.gov.au, or GPO Box 5218, Sydney NSW 2001. The Data Breach Response Team will ensure the statement includes the following details:
  - the Law Society's identity and contact details;
  - a description of the Eligible Data Breach - the date of the breach, the date the Law Society detected the breach, the circumstances (e.g. any known causes), who has obtained or is

likely to have obtained access to the Personal Information and relevant steps about what the Law Society has taken to address the breach;
- the kind or kinds of Personal Information involved, including any sensitive Personal Information;
- the steps the Law Society recommends that individuals take in response to the breach - these should be practical and easy for the individuals to do (e.g. if financial information is lost, recommend individuals contact their financial institutions to put them on notice of any unauthorised activities); and
- if a third party is involved in the breach, the statement may also include the contact details of the party who is not in charge of the notifications, or the fact that that third party is involved.

- **Notifying the affected individuals**
  Notification should be provided to individuals as soon as practicable after completing the statement for the Privacy Commissioner. The Data Breach Response Team will determine whether to contact individuals by telephone, SMS, physical or electronic mail, as long as it is reasonable in the circumstances. It will also consider which individuals to notify:

  - **Option 1 - Notify all individuals**
    This will be necessary if the Data Beach Response Team cannot assess which individuals are at risk, but it determines that some individuals are likely to suffer serious harm.

  - **Option 2 - Notify only those individuals at risk of serious harm**
    If the Data Breach Response Team can specifically identify the individuals who are likely to suffer serious harm, it will contact those individuals only.

  - **Option 3 - Publish notification**
    If neither of the above options are practicable, the Data Breach Response Team will ensure the statement is published on the Law Society website and it will take reasonable steps to publicise the statement, such as ensuring it can be indexed by search engines, publishing an announcement on the Law Society's social media or other communication channels, or taking out a print or online ad in publications or third party websites which the Law Society reasonably believes will reach the affected individuals.

- **Consider who else (other than the affected individuals) should be notified**
  The Data Breach Response Team must also consider what, if any, other stakeholders should be notified, such as other regulators or government agencies, insurers; and any other parties to which the Law Society has a contractual obligation to notify.

(4) **Prevent future breaches**

After an actual or suspected data breach has been resolved, the Data Breach Response Team will conduct a review of its data breach response procedures, which will include:

- reviewing the implementation of this policy;
- assessing the controls and systems in place in order to prevent similar incidents occurring in the future;
- advising any affected individual of the steps being taken to prevent similar incidents occurring in the future;
- carrying out a security audit of both physical and technical security;
- reviewing employee selection and training practices;

- reviewing service providers (e.g. offsite data storage providers); and
- keeping a record of the breach and the Law Society's management of it.

(f) Training

The Data Breach Response Team must provide Law Society Staff Members with:

- a copy of this policy; and
- the necessary training to enable the Law Society Staff Members to perform their obligations under this policy.

(g) Review

This Data Breach Response Policy will be reviewed:

- following any actual or suspected data breach;
- after the first 12 months of implementation; and
- thereafter every 12 months.

11. DEFINITIONS

Anti-Virus
Software that detects, repairs, cleans, or removes virus-infected files from a computer.

Audit
Independent external evaluation that clarifies whether the quality assurance system meets objectives, is efficient and fit for its purpose.

Authentication
A security method used to verify the identity of a user and authorise access to a system.

Authentication
A security method used to verify the identity of a user and authorise access to a system.

Bandwidth
A rate of data transfer, throughput or bit rate, measured in bits per second (bps).

Biometrics
Ccomprises methods for uniquely recognising humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Blogging
The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

BYOD
Any mobile technical device or equipment that is not owned by The Law Society of NSW e.g. mobile device.

Chain-Of-Custody
The chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.

Compromise
Exposure to threats either internal or external.

Confidentiality
Carried out or revealed in the expectation that anything done or revealed will be kept private.

Cross Cut Shredding
Safe and secure way of shredding paper documents.

Data
Information, e.g. numbers, text, images, and sounds, in a form that is suitable for storage in or processing by a computer.

Data Centre
A facility used to house computer systems and associated components.

Demilitarised Zone (DMZ)
A computer host or small network inserted as a "neutral zone" between the Law Society's private network and the outside public network. It prevents outside users from getting direct access to a server that has the Law Society data.

Denial of Service (DoS)
An attempt to make a computer resource unavailable to its intended users.

Desktop
A display on a computer screen comprising background and icons representing equipment, programs, and files.

Download
To transfer or copy data from one computer to another, or to a disk or peripheral device, or be transferred or copied in this way.

Downtime
Time during which work or production is stopped, e.g. because machinery is not working.

Email
Electronic mail, commonly called email or e-mail, is a method of exchanging digital messages across the Internet or other computer networks.

Encryption
The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Environment
The natural world regarded as being at risk from the harmful influences of human activities.

Event Logging
Event logging provides system administrators with information useful for diagnostics and auditing.

File Directories
A virtual container within a digital file system, in which groups of computer files and other folders can be kept and organised.

File Sharing
The practice of distributing or providing access to digitally stored information, such as computer programs, multi-media (audio, video), documents, or electronic books.

Firewall
A firewall is a part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.

Guest
Any person who accesses the Law Society's IT Network who is not an employee of the Law Society. For the avoidance of doubt, this includes the non-employed elected representatives and councillors of the Law Society.

Hack
To use a computer or other technological device or system in order to gain unauthorised access to data held by another person or organisation.

Hardware
The equipment and devices that make up a computer system as opposed to the programs used on it

Identity Theft
A form of fraud in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name.

Information Technology
The study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware.

Infrastructure
The basic structure or features of a system or organisation.

Instant Messaging (IM)
Form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet. More advanced instant messaging software clients also allow enhanced modes of communication, such as live voice or video calling.

Intrusion Prevention System (IPS)
Network security appliances that monitor network and/or system activities for malicious activity. The main functions of "'intrusion prevention systems"' are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity.

IT Network
The Law Society's computer and information technology network, which is made up of the Law Society's servers, computers, routers and infrastructure, private intranet, public internet website, and any offsite or cloud storage.

Keycard
A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

Keypad
A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.

Login
The process of performing the necessary actions to start using a computer program or system

Malware
Short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent.

Mechanism
Device consisting of a piece of machinery: has moving parts that perform some function.

Mobile Data Device
A data storage device that utilises flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Network diagram
A schematic depicting the nodes and connections amongst nodes in a computer network or, more generally, any telecommunications network.

Network
Group of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources. Networks may be classified according to a wide variety of characteristics.

Packet Sniffing
Computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyses its content according to the appropriate RFC or other specifications.

Packet
A formatted unit of data carried by a packet mode computer network.

Passphrases
A sequence of words or other text used to control access to a computer system, program or data.

Password
A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

PDA
Stands for Personal Digital Assistant. A portable device that stores and organises personal information, such as contact information, calendar, and notes.

Peer-to-Peer (P2P) File Sharing
A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Personal Information
Information or an opinion about an identified individual, or an individual who is reasonably

identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

Phishing
The fraudulent practice of sending emails purporting to be from a reputable source in order to induce individuals to reveal confidential information, such as passwords and credit card numbers.

Real Time
The study of computer systems which are subject to a real-time constraint.

Reasonable Person
An ordinary and prudent person who normally exercises due care.

Reasonable Steps
All steps that are appropriate in the circumstances.

Redundancy
The duplication of critical components of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe.

Remote Access Policy
Document which outlines and defines acceptable methods of remotely connecting to the internal network. It is essential in large organisation where networks are geographically dispersed and extend into insecure network locations such as public networks or unmanaged home networks. It should cover all available methods to remotely access internal resources.

Remote Desktop Access
Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Router
An electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them.

Security Information Event Management (SIEM)
SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes.

Security Operations Centre (SOC)
A centralised unit in an organisation that deals with security issues, on an organisational and technical level.

Server
A server application, operating system, computer, or appliance.

Service Level Agreement's
Part of a service contract where the level of service is formally defined.

Service provider
An entity that provides services to other entities.

Smartphone
A mobile telephone that offers additional applications, such as PDA functions and email.

Software
Collection of computer programs and related data that provide the instructions telling a computer what to do.

Spyware
A type of malware that can be installed on computers and collects little bits of information at a time about users without their knowledge. The presence of spyware is typically hidden from the user, and can be difficult to detect. Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spywares such as keyloggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users.

Staff Member
Any staff member, employee, contractor, councillor or other worker (as that term is defined in the Work Health and Safety Act 2011 (NSW)) of the Law Society. References to "you" in this policy are references to you as a Staff Member.

Streaming Media
Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

Surge-Protectors
Protects electronics from power surges in the electrical system.

Switches
A computer networking device that connects network segments.

Transmission/Transmitting
The process of sending, propagating and receiving an analogue or digital information signal over a physical point-to-point or point-to-multipoint transmission medium, either wired or wireless.

Trojan
Also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbours a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.

Two Factor Authentication
Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorised, such as a security code.

Uninterruptible Power Supplies (UPSs)

A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically, also contains power surge protection.

Virtual Private Network (VPN)
A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network.

Virus
Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

WEP
Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

Wireless Access Point (WAP)
A device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth or related standards.

WPA
Stands for Wi-Fi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

ANNEXURE A: Notice of Computer Surveillance, Monitoring and Security Testing

The Law Society gives Notice that:

- it undertakes monitoring, surveillance and security testing of its IT Network, via software or other equipment of the Law Society's servers, desktop computers, routers and infrastructure, private intranet, public internet website, and any offsite or cloud storage;
- the monitoring, surveillance and security testing is undertaken in accordance with the Law Society's *IT Security and Privacy policy* (available for review on the Law Society's intranet/portal), in order to ensure continued compliance with the Policy;
- the monitoring, surveillance and security testing extends to any computer, smartphone or other device that accesses the IT Network or data, as well as the contents of any removable media (such as USB drives) that is loaded onto the IT Network;
- the data and information subject to monitoring, surveillance and security testing includes but is not limited to:
    - websites visited and cookies stored from those websites;
    - emails sent and received using the Law Society's email server;
    - files (whether uploaded, downloaded or stored);
    - information posted on social network and blogging websites;
    - messages and other data;
    - metadata from files opened and saved;
- any persons using the Law Society's IT Network to send, receive or access the forms of data listed above should expect no privacy as a consequence of the Law Society's monitoring, surveillance and security testing systems;
- the monitoring, surveillance and security testing will commence fourteen (14) days following the date this Notice is given; and
- the monitoring, surveillance and security testing will be continuous – meaning that it will be ongoing.

ANNEXURE B: Boot Notice of Computer Surveillance and Monitoring

The Law Society gives Notice that it undertakes monitoring, surveillance and security testing of its IT Network (including this computer) in accordance with the Law Society's *IT Security and Privacy Policy* (available for review on the Law Society's intranet/portal), in order to ensure continued compliance with the Policy.

This monitoring, surveillance and security testing includes, but is not limited to: the websites visited and cookies stored from these websites; emails sent and received using the Law Society's email server; files (whether uploaded, downloaded, accessed or stored); and any removable media (such as USB drives) that are loaded onto the IT Network.

This monitoring, surveillance and security testing will be continuous – meaning that it will be ongoing.

ANNEXURE C: Guest - Acceptable Use and Computer Surveillance Notice

Guest Access to IT Network

The Law Society provides guests with access to the IT network as a courtesy, or to any person who can demonstrate a reasonable business need to access the IT Network, or a reasonable business need to access the Internet via the Law Society IT Network

Acceptable Use

Guests must ensure their use of the Law Society's IT Network (including its bandwidth) and other computer resources is reasonable. Guests who use the Law Society's IT Network to download large files or stream movies or music may have their guest access revoked.

Unacceptable Use

Guests must not use the Law Society's IT Network in order to:

- disseminate or access any defamatory, discriminatory, vilifying, abusive, threatening, offensive, pornographic or otherwise inappropriate or unlawful websites, material or media;
- download, install or use unauthorised software or programs;
- engage in activities that cause an invasion of privacy;
- perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques;
- install or distribute unlicensed or "pirated" software; or
- engage in activity that is illegal under local, state, federal, or international law;

Notice of Computer Surveillance, Monitoring and Security Testing

Guests are to be aware that:

- the Law Society undertakes monitoring, surveillance and security testing of its IT Network, via software or other equipment of the Law Society's servers, desktop computers, routers and infrastructure, private intranet, public internet website, and any offsite or cloud storage;
- the monitoring, surveillance and security testing is undertaken in accordance with the Law Society's *IT Security and Privacy Policy* (available for review on the Law Society's intranet/portal), in order to ensure continued compliance with the Policy;
- the monitoring, surveillance and security testing extends to any computer, smartphone or other device that accesses the IT Network or data, as well as the contents of any removable media (such as USB drives) that is loaded onto the IT Network;

- the data and information subject to monitoring, surveillance and security testing includes but is not limited to:
    - websites visited and cookies stored from those websites;
    - emails sent and received using the Law Society's email server;
    - files (whether uploaded, downloaded or stored);
    - information posted on social network and blogging websites;
    - messages and other data;
    - metadata from files opened and saved;
- the monitoring, surveillance and security testing will be continuous – meaning that it will be ongoing.

Acceptance of Terms and Conditions

By signing below, I confirm that:

- I have requested guest access to the Law Society's IT Network;
- I have received and reviewed the Law Society's Acceptable Use and Computer Surveillance Notice (i.e. this Notice); and
- I have read, understood and agree to the terms of the Notice.

_____

Signature of Guest

_____

Name of Guest

_____

Date

ANNEXURE D: Deed relating to the use of Law Society Mobile Services on BYOD(s)

This Deed Poll is given by _____(**the Staff Member**) in favour of the Law Society of New South Wales (**the Law Society**).

Background

A. The Staff Member wishes to utilise their own mobile Information Technology device(s) (**BYOD(s)**) in the course of performing their duties for the Law Society, being a BYOD(s) owned or operated by the Staff Member (whether purchased by the Staff Member or with the Law Society's financial assistance).

B. The Law Society has given its approval for the Staff Member to use the Staff Member's BYOD(s) for business purposes, subject to the Staff Member's agreement to:

(a) the provisions of this Deed Poll; and

(b) the *Law Society's IT Security and Privacy Policy*, to which the form of this Deed Poll is an Annexure (the **Policy**).

General terms

1. The Staff Member agrees to comply with the provisions of this Deed Poll and the Policy as varied from time to time, in relation to the BYOD(s) and the applicable Mobile Plan.

Security of Systems and Device(s)

2. The Staff Member will do all things required by the Law Society from time to time, and otherwise take reasonable steps, to protect the security, integrity and confidentiality of any data or material associated with the Law Society that is stored on, or accessible by, the BYOD(s);

3. The Staff Member will allow and do all things reasonably necessary to enable the Law Society to install software on the BYOD(s) (the **Installed Software**), to safeguard and protect the Law Society against viruses or any other incident occurring that could otherwise damage or compromise the Law Society IT Networks and IT System (the **Systems**).

4. The Staff Member acknowledges and agrees that the Staff Member has no right or claim of any kind against the Law Society for any loss or damage caused to the BYOD(s) or software contained on it arising directly or indirectly from the installation, operation or effect of the Installed Software, unless and to the extent that any such loss or damage is caused by the negligence or wilful misconduct of the Law Society.

5. The Staff Member must immediately report the following events to their Manager and the Manager of the IT Department:

5.1. the BYOD(s) is lost, misplaced, damaged or stolen; or

5.2. the Staff Member becomes aware of any risk to the Systems arising from the BYOD(s).

6. If a BYOD is lost or stolen, the Staff Member agrees to follow all directions from the Law Society in respect of the lost BYOD, which may include:

   6.1. using remote management facilities to lock or destroy all data on the BYOD;

   6.2. instructing any third-party network operator to render the BYOD inoperable; and

   6.3. co-operating with police or other authorities to report on the loss of the BYOD, and assist with any investigation into the loss.

7. The Staff Member will make the BYOD(s) available for inspection by an authorised officer of the Law Society, when reasonably required by the Law Society and upon reasonable request, and only for the purposes of determining that:

   7.1. it contains the Installed Software and that the Installed Software is operating effectively; or

   7.2. the BYOD(s) otherwise complies with this Deed and the Policy.

8. As the BYOD(s) is linked to the Systems, it must be secured by the Staff Member at all times via a PIN and/or password.

9. The Staff Member acknowledges and agrees that they are solely responsible for the care and security of the BYOD(s) and that the Law Society will not be liable for any theft, loss or damage caused to the BYOD(s), unless and to the extent that any such theft, loss or damage is caused by the negligence or wilful misconduct of the Law Society.

Staff Member acknowledgements

10. The Staff Member acknowledges and agrees as follows:

    10.1. they have read and understood the Policy and it applies to their employment or engagement with the Law Society;

    10.2. they have had the opportunity to raise any questions about this Deed Poll and the Policy with the Law Society and to seek their own advice;

    10.3. this Deed Poll and the Policy are necessary for the purposes of the Law Society carrying out its functions and the Staff Member using a BYOD(s) in the workplace to perform their role;

    10.4. any non-compliance with this Deed Poll or the Policy may result in disciplinary action which, in the case of material non-compliance, may include the termination of the Staff Member's employment or engagement with the Law Society;

    10.5. the Law Society will not be responsible for the provision of any technical support regarding the BYOD(s)and

    10.6. the Staff Member will continually maintain the security or the BYOD by applying the latest operating system and patch updates within seven (7) days of such updates becoming available.

On Leaving the Law Society

11. The Staff Member must ensure that all Law Society data is removed from the BYOD(s) when the Staff Member's employment or engagement with the Law Society ends, and the Staff Member acknowledges that any failure to do so risks all data stored on the device, whether personal or related to Law Society business.

12. The Staff Member authorises the Law Society IT Department to remove any work related data or information (including but not limited to contacts, mail, calendar and files) from the BYOD(s) when the Staff Member's employment or engagement with the Law Society ends. This removal of data and information may be conducted remotely and without notice by the IT Department on or after the Staff Member's leave date.

13. The Staff Member may contact the IT Department prior to leaving the Law Society to request the removal of "Active Sync" settings on the BYOD(s) which have been so configured, so as to minimise any loss of data or information. The Law Society will not be responsible for any loss of data or information from the BYOD(s) which occurs after the Staff Member's employment or other engagement with the Law Society is terminated or otherwise ceases.

EXECUTED as a Deed Poll in Sydney

Executed by the Staff Member:

.....	.....
Name	
Signature	Witness
Date	

ANNEXURE E: Employee data breach response policy

This Employee Data Breach Response Policy identifies the procedures that all Law Society Staff Members must follow in the event of a known or suspected data breach.

(a) Key Concepts

Data Breach Response Team means the individuals identified in Annexure G to this Policy.

Eligible Data Breach is a data breach which:

- involves unauthorised access to, disclosure of, or loss of, Personal Information held by the Law Society; and
- is likely to cause serious harm to the affected individuals, determined on an objective assessment from the viewpoint of a Reasonable Person in the Law Society's position.

(b) Your responsibilities

(1) Duty to report

If you discover, suspect or are notified about a known or suspected data breach, you must report such incident to the General Counsel of the Law Society and no other person (unless subsequently authorised by the General Counsel) immediately, as the Law Society is required to make a reasonable and prompt assessment within 30 days.

The General Counsel, Meaghan Lewis (at the time of writing), may be contacted at: (02) 9926 0321 or meaghan.lewis@lawsociety.com.au. Please include the words "Privileged and Confidential" in the subject or heading of any communications with the General Counsel in relation to the incident.

An email template form of reporting to the General Counsel is set out in **Annexure F**.

Do not notify any other person of the incident unless specifically instructed by the General Counsel.

An illustrative but non-exhaustive list of events which, by their very nature, probably give rise to the duty to report to the General Counsel follows:

- theft or loss of a laptop, USB or other data storage device owned by the Law Society containing Personal Information;
- a break-in or robbery at the Law Society office;
- a computer hacker compromising the Law Society's databases, networks or communications containing Personal Information;

- a Law Society Staff Member accessing or disclosing Personal Information outside the requirements or authorisation of their employment;
- theft of paper records from unsecured recycling or garbage bins; or
- a Law Society Staff Member mistakenly providing Personal Information to the wrong person (e.g. sending member information to the wrong recipient, or providing employee salary or other Personal Information to the wrong employee).

(2) Duty to preserve evidence

If any laptop or device owned by the Law Society is hacked or accessed in an unauthorised way, you must terminate the network or wireless connection, but do not turn the laptop or device off. This may enable the General Counsel and Data Breach Response Team to preserve important evidence and information relating to the data breach.

(3) Duty to cooperate and assist

Law Society Staff Members must cooperate with the General Counsel and the Data Breach Response Team in relation to any investigation into a known or suspected data breach and provide reasonable assistance to them.

(4) Duty to maintain confidentiality

Law Society Staff Members must not disclose the known or suspected data breach, or any information about any such incident, within or outside the Law Society, other than to the General Counsel, until expressly authorised by the General Counsel to do so.

(c) Acknowledgement

This Employee Data Breach Response Policy does not create any rights for Law Society Staff Members or any rights outside the scope of the Law Society's obligations under applicable law. It is confidential and internal to the Law Society and shall not create any rights or entitlements of any third parties either.

The Law Society Staff Members acknowledge and agree the contents of this policy and will act in accordance with its terms as a condition of their employment with the Law Society.

ANNEXURE F: Email template for reporting data breaches

PRIVILEGED AND CONFIDENTIAL

Dear Meaghan,

I am emailing you to report a potential data breach pursuant to the Law Society's employee data breach response policy. I understand that this incident may have legal consequences and you need to advise the Law Society on those matters. I have, accordingly, addressed this report only to you.

[[Between/On] [IDENTIFY TIME PERIOD OF BREACH], [SUMMARISE WHAT YOU KNOW OF THE DATA BREACH].]

The data accessed [may have included/included] personal information such as [IDENTIFY TYPES OF PERSONAL IDENTIFICATION INFORMATION AT ISSUE (IF KNOWN)].

Please contact me on [insert details] to if you wish to discuss or if you require any further details or information.

[SIGNOFF]

ANNEXURE G: Data Breach Response Team's roles and responsibilities

A. Data Breach Response Team

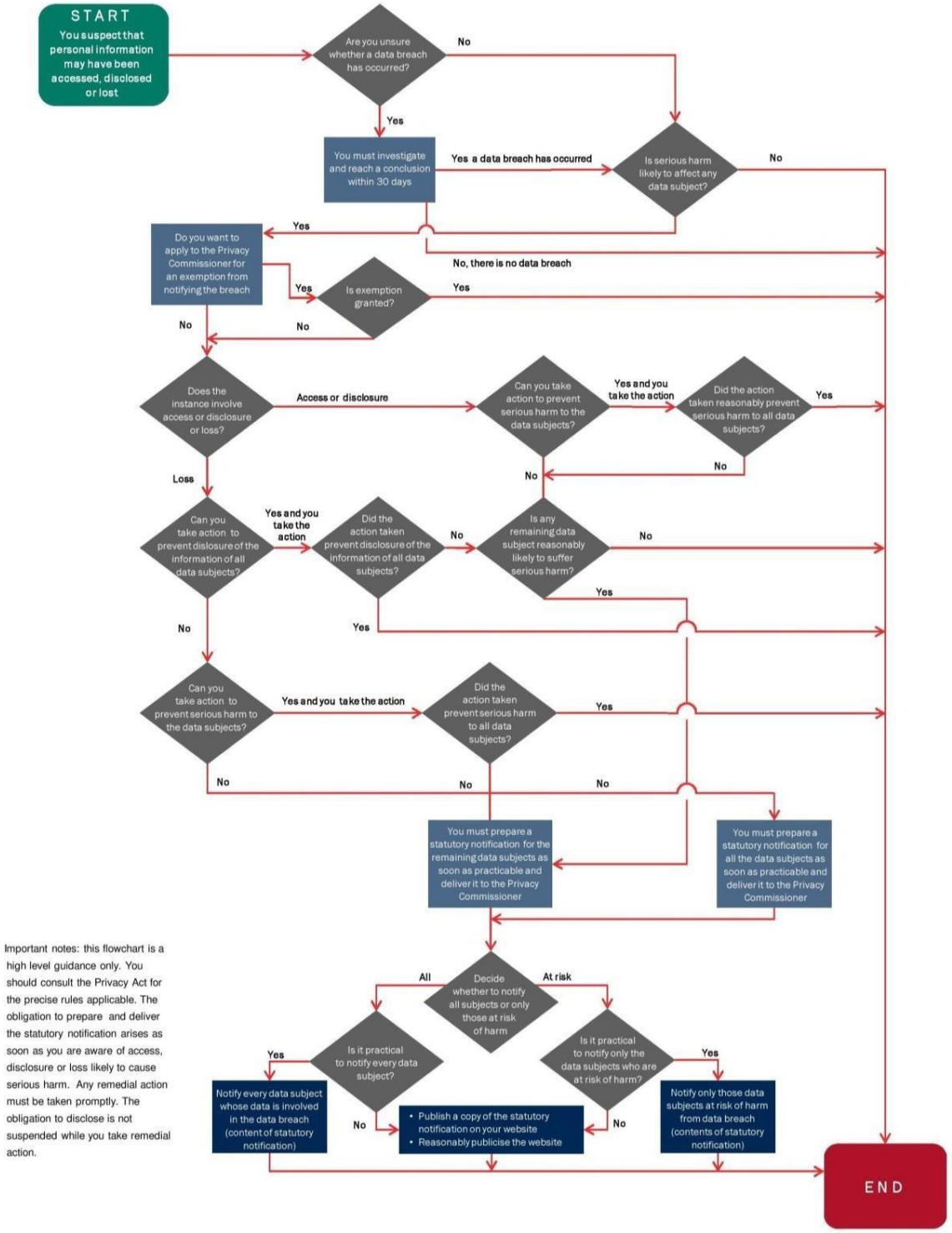
Position	Name	Contact details
General Counsel (and Team Leader)	Meaghan Lewis	T: (02) 9926 0321 M: 0498 200 023 E: meaghan.lewis@lawsociety.com.au
Privacy Officer	Meaghan Lewis	T: (02) 9926 0321 E: meaghan.lewis@lawsociety.com.au
Chief Operating Officer	Kenneth Tickle	T: (02) 9926 0234 E: kenneth.tickle@lawsociety.com.au
Head of IT	Lee Bustin	T: (02) 9926 0150 M: 0408 236 674 E: lee.bustin@lawsociety.com.au
Media and Public Relations Manager	Damien Smith	T: (02) 9926 0288 M: 0413 440 699 E: damien.smith@lawsociety.com.au
Head of Marketing and Communications	Claire Chaffey	T: (02) 9926 0393 E: claire.chaffey@lawsociety.com.au
Director, Professional Standards	Anthony Lean	T: (02) 9926 0307 E: anthony.lean@lawsociety.com.au
Head of Human Resources	Regina Elias	T: (02) 9926 0205 E: regina.elias@lawsociety.com.au
Quality Assurance and Audit	Margaret Bowman	T: (02) 9926 0353 E: margaret.bowman@lawsociety.com.au
Paralegal assistance	Patricia Cillo	T: (02) 9926 0159 E: patricia.cillo@lawsociety.com.au

B. Roles and Responsibilities

The General Counsel will act as the Team Leader of the Data Breach Response Team. As soon as reasonably practicable after the General Counsel is notified about a data breach (suspected or known), the General Counsel will schedule a kick-off meeting for the Data Breach Response Team. In that meeting the General Counsel will be responsible for delegating the following actions to one or more members of the Data Breach Response Team (as the context requires):

Action
Determine what laws apply to the data breach • Involve outside counsel as necessary to implement the Policy
Determine whether suspected data breach is an "eligible data breach" • Take all reasonable steps to carry out assessment within 30 days of becoming aware of reasonable grounds for suspicion
Investigation and analysis • Investigate the data breach and gather additional information to assess risk • Where appropriate, work with law enforcement or third-party investigators
Containment and recovery • Take all necessary steps to contain the impact of the data breach • Work with other departments to ensure the breach remains confidential until notification decisions have been made
Remedial action • Where possible, take effective remedial action before serious harm is caused
Notification statement • Provide a compliant statement to the OAIC and to any affected individuals • Publish a copy of the notification statement on website and take reasonable steps to publicise (if it is not possible to notify all affected individuals)
Assessment and review • Review data breach response procedures and implementation of the Data Breach Response Policy
Staff training • Ensure regular staff training in relation to the Employee Data Breach Response Policy and best data security practices
Policy review • Review the Data Breach Response Policy every 12 months

ANNEXURE H: Flowchart of procedures to follow in case of a data breach



ACKNOWLEDGEMENT OF POLICY

By signing below, I confirm that:

- I have been given a copy of the Law Society's **IT Security and Privacy Policy**;
- I was instructed to read the policy and raise any questions I had in relation to it with the Practice Manager;
- I have since read and understood the policy;
- I agree to be bound by the policy;

_____

Signature

_____

Name

_____

Date